SZKOŁA GŁÓWNA HANDLOWA
Studium Dyplomowe

HANDEL ELEKTRONICZNY (ELECTRONIC COMMERCE) - PŁATNOŚCI POPRZEZ INTERNET

Marek Ryfko
nr alb. 602

Praca magisterska napisana pod kierunkiem
prof. dr hab. Jana Golińskiego

Katedra Informatyki Gospodarczej

WARSZAWA 1996

Spis treści

WST□P

Dzisiejszy świat biznesu charakteryzuje się globalną konkurencją. Zwyciężają firmy najszybciej reagujące na zmieniające się potrzeby swoich klientów i sytuację na rynku. Kluczem do powodzenia jakiejkolwiek poważnej działalności gospodarczej staje się informacja, sposób jej pozyskiwania, używania, przechowywania i przesyłania. Technologia informatyczna odgrywa tu zasadniczą rolę. Jej zastosowanie rośnie wraz z rozwojem różnego typu sieci komputerowych, wśród których największe znaczenie ma Internet- sieć sieci i zaczątek globalnej Infostrady.

Infostrada to bardzo szybkie sieci cyfrowe, mogące transmitować dane, dźwięk, grafikę, animację. Oczekuje się, że do roku 2010 większość transakcji handlowych zawierana będzie za ich pośrednictwem. Zmieni się także sposób wyszukiwania informacji, uczenia się, leczenia, odpoczywania. Infostrada będzie miała wpływ na wszystkie aspekty życia.

Wraz z wynalezieniem globalnej pajęczyny World Wide Web, Internet stał się atrakcyjny i wystarczająco prosty w użyciu, by mógł posługiwać się nim przeciętny użytkownik. Eksplozja jego popularności (ponad 40 mln użytkowników i ich podwajanie się co 12 miesięcy) sprawiła, że Internet stał się bardzo atrakcyjnym medium dla świata biznesu. Może służyć do wymiany informacji i bezpośredniego handlu towarami i usługami.

Wykorzystanie Internetu do celów handlowych jest hamowane uwarunkowaniami technologicznymi. Internet jest siecią otwartą, do której każdy może się przyłączyć i w której nie ma jednego właściciela. Internet często określa się przymiotnikiem „anarchiczny", gdyż opiera się na wzajemnym zaufaniu użytkowników i ich odpowiedzialności. Ten model sprawdzał się początkowo, gdy Internet wykorzystany był głównie przez ośrodki badawcze i uniwersytety. Wymagania biznesu są jednak inne, gdyż prowadzenie handlu wymaga bezpieczeństwa transakcji, poufności informacji, sprawdzonych mechanizmów dokonywania płatności. Bez spełnienia tych warunków właściciele praw intelektualnych i wszyscy, którzy mogliby zacząć sprzedawać w sieci swoje wartościowe usługi i towary, nie będą mieli ku temu wystarczającej motywacji.

W elektronicznym handlu poprzez Internet występuje szereg następujących po sobie etapów: dotarcie z informacją do klienta, o ile to możliwe dostarczenie mu siecią żądanej usługi i przyjęcie tą samą drogą płatności. Tematem pracy jest omówienie komercyjnego zastosowania Internetu ze szczególnym uwzględnieniem istniejących i proponowanych mechanizmów umożliwiających bezpieczne płatności finansowe za pośrednictwem tej sieci.

Systemy internetowego handlu ewoluują wraz z rozwojem samego Internetu. Pierwsze zastosowania komercyjne rozpoczęły się ok. 3 lata temu, w tym systemy internetowych płatności stosuje się od ok. 2 lat. Obecnie oferowana jest cała gama różnych rozwiązań. Ze względu na bardzo szybkie tempo ich zmian i dojrzewania trudno jest uzyskać materiały na temat internetowych płatności w formie innej niż elektroniczna. Niewiele jest na ten temat książek, publikowane w czasopismach artykuły zwykle nie wykraczają poza ogólne omówienie problemu. Nie ma prawie żadnych poważnych źródeł w języku polskim. Gros informacji rozsianych jest w postaci elektronicznej po całej sieci Internet.

Praca ta powstała głównie na podstawie materiałów anglojęzycznych dostępnych w sieci Internet. Z tego powodu w bibliografii i odnośnikach autor podaje adresy internetowe w znormalizowanej konwencji URL (Universal Resource Locator).

Pierwszy rozdział definiuje pojęcia Internetu i handlu elektronicznego oraz omawia problematykę komercyjnego zastosowania Internetu, jego wykorzystania w bankowości i handlu detalicznym.

Rozdział drugi stanowi przegląd obecnie oferowanych bezpiecznych metod płatności poprzez Internet.

Rozdział trzeci omawia kwestie bezpieczeństwa danych przesyłanych poprzez Internet i umożliwia pełniejsze zrozumienie sposobu funkcjonowania internetowych mechanizmów płatności.

1. HANDEL ELEKTRONICZNY

1.1. CZYM JEST INTERNET?

Internet bardzo szybko staje się dominującą platformą wymiany informacji. Czym właściwie jest Internet? Krol i Hoffman[1] podają następujące 3 uzupełniające się definicje:

1. sieć sieci opartych na protokole TCP/IP
2. wspólnota ludzi którzy użytkują i tworzą te sieci
3. kolekcja zasobów dostępnych przez te sieci

W warstwie technicznej najważniejszy jest fakt, że powiązane ze sobą sieci porozumiewają się za pośrednictwem wspólnego protokołu TCP/IP. Protokół sieci jest językiem wymiany danych pomiędzy tworzącymi ją komputerami. Dodatkowo Internet może komunikować się z sieciami zbudowanymi na podstawie innych protokołów.

W warstwie zasobów pod pojęciem Internet rozumie się wszystkie programy, informacje i usługi jakie możemy w Internecie znaleźć. Do sprecyzowania gdzie są te zasoby i jaki jest do nich dostęp podaje się ich adres. Z czasem wytworzyła się znormalizowana postać adresowania. Wskazuje się je poprzez URL czyli Universal Resource Locator. Ma on postać „protokół://adres_komputera/ścieżka_dostępu/nazwa_pliku”. Najpopularniejsze obecnie protokoły to : http, news, gopher, telnet, file, ftp, wais. Oznaczają one poszczególne usługi sieci Internet. Przykładowy adres URL to http://www.vol.it/EDICOLA/ZYCIE/DATA/ pod którym mieści się elektroniczne wydanie Życia Warszawy.

Internet narodził się w USA w latach sześćdziesiątych jako rozwinięcie rządowego projektu ARPANET- eksperymentalnej sieci na potrzeby badań militarnych. Jej cechą miało być zachowanie zdolności komunikacyjnych w warunkach konfliktu nuklearnego, czyli potencjalnego zniszczenia części węzłów sieci.

ARPANET opracowano w ten sposób, by nie był konieczny żaden centralny punkt sterowania, którego wyłączenie uniemożliwiałoby pracę pozostałej części sieci. Wszystkie węzły (komputery) zostały równouprawnione. Indywidualnie wysyłały, odbierały i przesyłały wiadomości. Wiadomości podzielone zostały na pakiety, z których każdy adresowany był oddzielnie. Pakiety na własną rękę poszukiwały sposobu dotarcia do odbiorcy. Jeżeli jedna droga była zamknięta, usiłowały znaleźć alternatywną. Taka architektura powodowała wysoką odporność sieci na zaburzenia pracy poszczególnych części składowych.

Wspólny protokół łączący sprzęt różnych producentów okazał się dobrym pomysłem- sieć pracowała nad wyraz stabilnie. Szybko okazało się, że chociaż sieć ARPANET stworzona została głównie w celu udostępnienia naukowcom mocy obliczeniowej tworzących ją komputerów, to najpopularniejszą usługą stały się różne formy poczty elektronicznej. Posługiwano się nią w celu wymiany informacji, często nie związanych z pracą. Sieć została wkrótce udostępniona uniwersytetom, ośrodkom badawczym i agendom rządowym. Zaczęto ją nazywać Internetem.

Z czasem do Internetu zaczęli podłączać się użytkownicy ze sfery komercyjnej. Obecnie większość z podsieci składających się na Internet jest w rękach prywatnych. Analogicznie jak Internet sposób funkcjonowania ma globalna telefonia. Systemy telefoniczne poszczególnych państw są w rękach niezależnych firm, ale poprzez wspólne standardy transmitują one między sobą rozmowy użytkowników.

Najczęściej wykorzystywaną usługą Internetu jest poczta elektroniczna. Jest to bardzo pewna i tania metoda komunikowania się. Początkowo pocztą przesyłać można było tylko tekst. Z czasem wzbogacono go o zdjęcia, dźwięk, animację i dowolną inną informację w postaci cyfrowej. Przesłanie listu na inny kontynent zajmuje zwykle kilka sekund. Dla użytkownika koszt i sposób wysłania wiadomości jest taki sam niezależnie od odległości. Ponadto koszt przyłączenia do Internetu nie zależy zwykle od ilości generowanego ruchu, lecz tylko od przepustowości łącza. Zastosowanie Internetu zamiast tradycyjnej poczty, telefonu i faxu do komunikacji pomiędzy rozsianymi po całym świecie oddziałami korporacji potrafi znakomicie obniżyć koszty działalności.

[1] gopher://ds1.internic.net/00/fyi/fyi20.txt

Inną bardzo popularną usługą internetową jest USENET- system grup dyskusyjnych. Jest ich tysiące i poświęcone są całej gamie tematów: komputerom, biznesowi, rozrywce, nauce etc. USENET działa na podobnej zasadzie jak poczta elektroniczna. Wysyłamy wiadomość, która czytana jest przez wiele osób. Łatwo jest również odpowiadać na czyjąś wiadomość, wysyłając listy zarówno do całej grupy, jak i do indywidualnych nadawców.

Innymi często używanymi usługami są ftp i telnet. Ftp umożliwia przesyłanie plików pomiędzy komputerami, a telnet zdalną pracę na innych maszynach. Przykładowo, siedząc w domu, możemy poprzez telnet wejść na superkomputer firmy i pracować na nim tak jakbyśmy przy nim siedzieli.

Prawdziwą rewolucję w zastosowaniach Internetu przyniosło wynalezienie World Wide Web (WWW) - światowej pajęczyny. WWW został stworzony w laboratoriach instytutu badań jądrowych CERN[2]. Przez zastosowanie graficznych przeglądarek zasoby Internetu stanęły otworem dla szerokiego grona użytkowników, których początkowo zniechęcał skomplikowany sposób poruszania się po sieci.

Strony WWW mogą zawierać bogato formatowany tekst, grafikę, muzykę w tle, animację i hipertekst- połączenia z innymi stronami, które mogą być zlokalizowane na zupełnie innych, często odległych komputerach. Użytkownik po prostu wybiera te połączenia i automatycznie jest przenoszony do innego serwisu. Nie musi się troszczyć o pamiętanie adresów czy sposobów dotarcia do określonego miejsca. Może skoncentrować się na interesującej go treści.

Szybko opracowano specjalne silniki przeszukiwania zasobów WWW, korzystając z których łatwo zlokalizować interesującą nas informację. Pierwszą graficzną przeglądarką WWW był Mosaic stworzony przez NCSA (National Center for Supercomputing Applications) przy University of Illinois. Szybko stworzono następne, z których najpopularniejszą obecnie jest Netscape Navigator.

WWW stało się niewątpliwie najpopularniejszą obok poczty elektronicznej usługą Internetu. Dla przeciętnego użytkownika WWW jest wręcz tożsame z Internetem. Przeglądarki WWW integrują wszystkie usługi internetowe, często mówi się o nich jako o „super-aplikacjach". Obecnie trwają prace nad dodatkowym poszerzeniem ich możliwości, m.in. o pracę grupową i internetowy telefon. Przeglądarki WWW oferują bardzo naturalny, w zasadzie nie wymagający uczenia się sposób poruszania się po sieci. Większość mechanizmów handlu internetowego zbudowana jest na podstawie WWW.

[2] http://www.cern.ch/

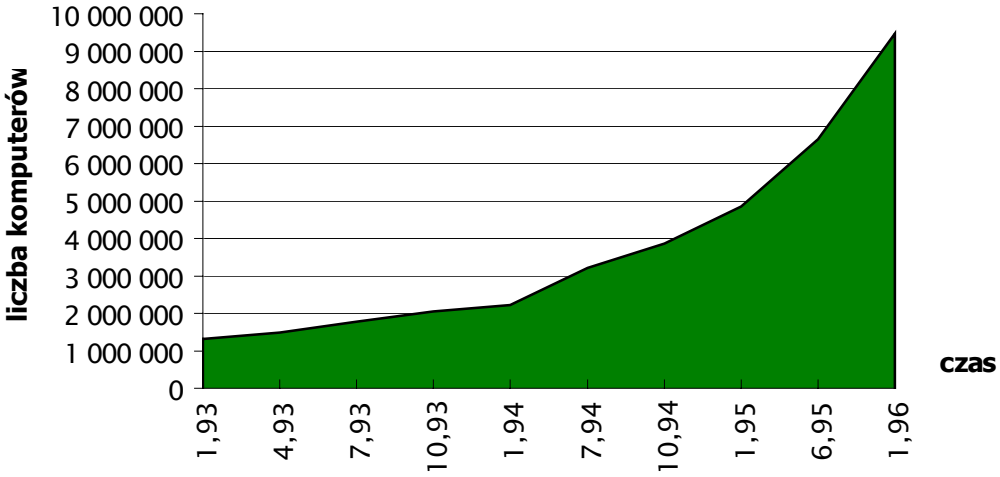
1.2. INTERNET- STATYSTYKA WZROSTU I WYKORZYSTANIA

Liczba osób korzystających z Internetu gwałtownie wzrasta. W jego wykorzystaniu przodują Amerykanie. W ich domach komputer stał się sprzętem codziennego użytku. Badanie przeprowadzone w styczniu 1996 przez Software Publishers Association[3] wykazały, że komputer osobisty posiada 34% amerykańskich gospodarstw domowych. 70% osób posiadających komputer ma jednocześnie modem, co stanowi wystarczającą kombinację sprzętową do posługiwania się Internetem. Ten sam sondaż wykazał, iż 8,4% amerykańskich gospodarstw domowych ma dostęp do WWW. Przy założeniu[4], że w każdym gospodarstwie domowym średnio 1,3 osoby korzysta z Internetu, można powiedzieć, że w Stanach Zjednoczonych z sieci korzysta ok. 10 milionów osób. Około 60%[5] procent użytkowników posługuje się nim także w pracy.

Jeszcze bardziej optymistyczne są wyniki badań przeprowadzonych przez CommerceNet Consortium/ Nielsen Media Research. Badania te wykazały, że dostęp do Internetu w USA i Kanadzie ma 37 milionów osób (17% całej populacji powyżej 16 lat). 24 miliony osób używało Internetu w ciągu ostatnich 3 miesięcy, z czego 18 milionów korzystało z WWW. Przeciętny użytkownik korzysta z Internetu 5 godzin i 28 minut tygodniowo.

[3] http://www.spa.org
[4] NPD Group, http://www.npd.com
[5] Emerging Technologies Research Group; http://etrg.findsvp.com/features/newinet.html

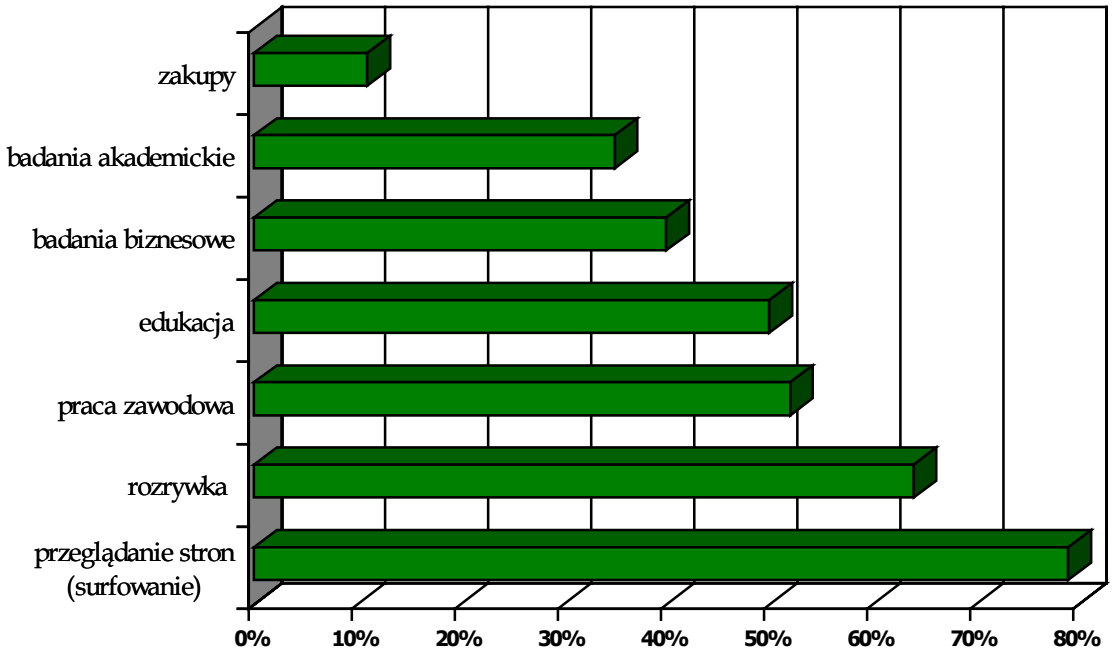
Jak rośnie liczba komputerów w sieci Internet?



Wykres A Wzrost ilości hostów internetowych (Źródło: Network Wizards; http://www.nw.com/zone/WWW/report.html).

Prognoza przewiduje, że do roku 2000 liczba komputerów bezpośrednio podłączonych do Internetu wzrośnie do 100 000.

Do czego wykorzystywane jest najczęściej WWW?

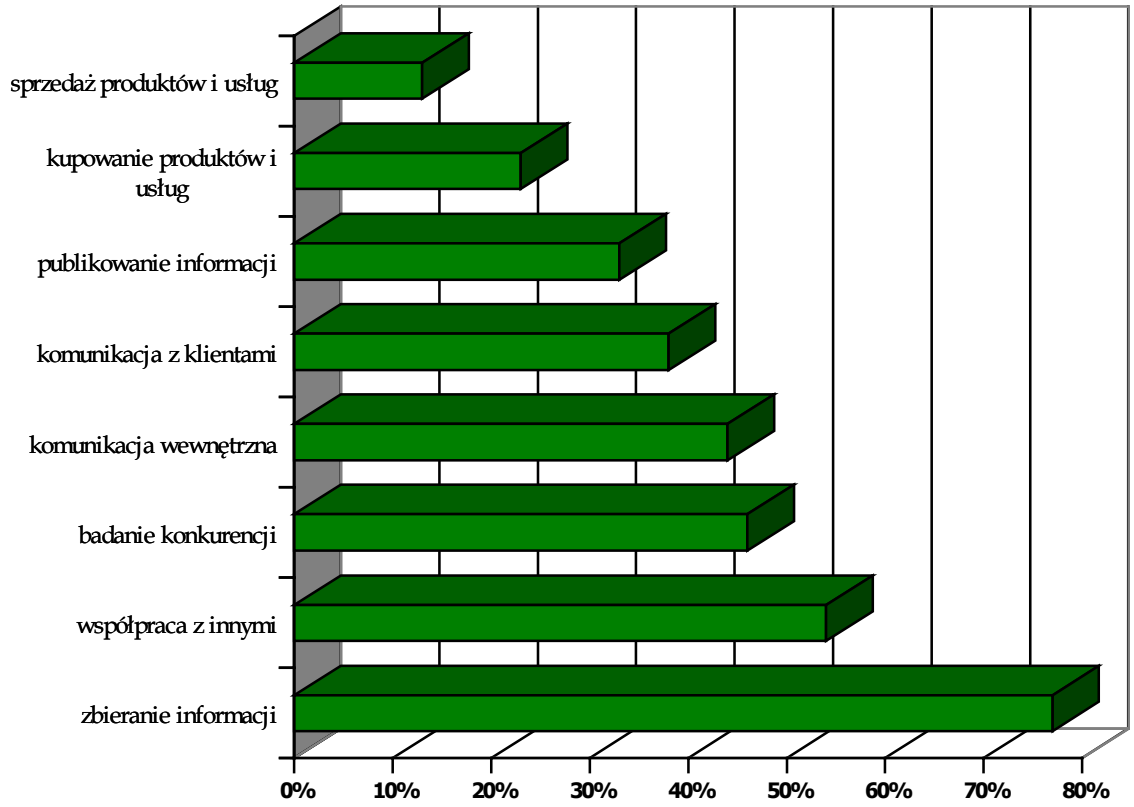


Wykres B Najpopularniejsze zastosowania WWW (Źródło: University of Michigan Business School 4th Consumer Survey of WWW Users).

Sondaże pokazują, że Internetem posługuje się grupa osób bardzo atrakcyjnych jako potencjalni konsumenci. Są to osoby zwykle ponadprzeciętnie zarabiające. 25% użytkowników WWW ma dochody ponad 80 000 USD (średnia amerykańska i kanadyjska o takich dochodach to 10% populacji). Użytkownicy Internetu/WWW są także bardzo dobrze wykształceni. 64% ma przynajmniej pierwszy stopień naukowy (łączona średnia amerykańska i kanadyjska to 29%).

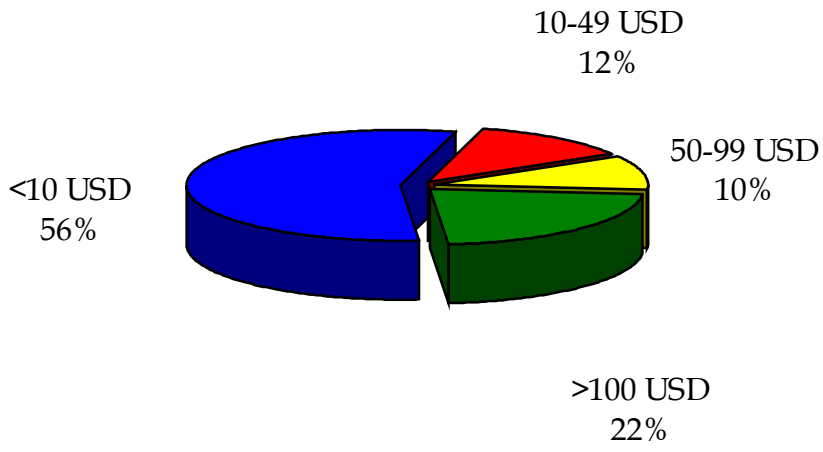
Ponad połowa użytkowników używała już WWW do pracy.

Najczęstsze zastosowania to:



Wykres C Zastosowanie WWW do pracy. (Źródło: CommerceNet Consortium/Nielsen Media Research 1995).

Handel za pośrednictwem Internetu stał się faktem. Badania CommerceNet Consortium/Nielsen Media Research pokazują, że ok. 2,5 miliona (14%) amerykańskich i kanadyjskich użytkowników WWW zakupiło za pośrednictwem Internetu jakieś produkty czy usługi. Wydatki użytkowników sieci w zależności od kosztu produktu/usługi kształtowały się w następujący sposób:

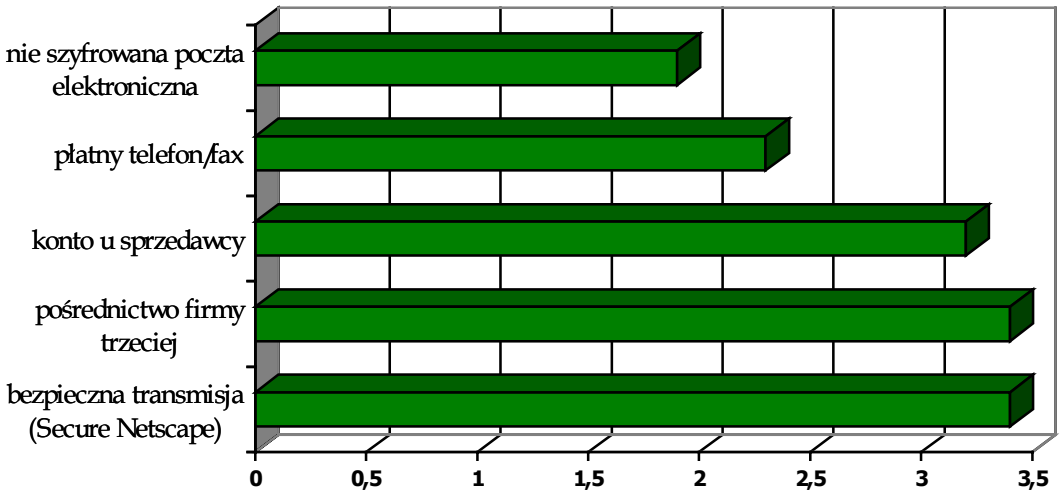


Wykres D Procentowa wartość całościowych wydatków użytkowników sieci w okresie ostatnich 6 miesięcy (Źródło: University of Michigan Business School 4th Consumer Survey of WWW Users).

Wg badań[6] University of Michigan Business School jako najważniejszą przeszkodę w używaniu WWW do robienia zakupów 60% respondentów wymienia bezpieczeństwo transakcji. Przesyłanie informacji o zakupie/płatności siecią jest uważane za bardziej ryzykowne niż przekazywanie jej w sposób konwencjonalny, tj. telefonicznie czy faxem.

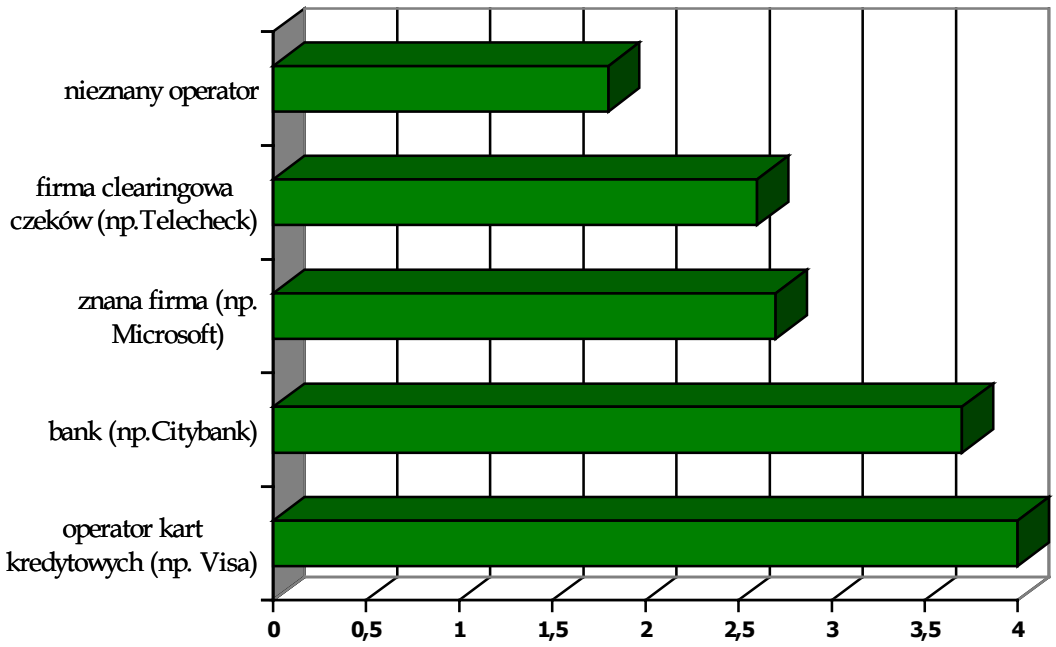
[6] 4th Consumer Survey of WWW Users; (http://www.cc.gatech.edu/gvu/user_surveys/survey-04-1995/)

Te same badania przynoszą następujące rezultaty, jeśli chodzi o preferencje użytkowników sieci odnośnie mechanizmów płatności za pośrednictwem Internetu (oceny są w skali 1 do 5, im bliżej 5, tym większe zainteresowanie):



Wykres E Preferencje użytkowników odnośnie mechanizmów płatności internetowych (Źródło: 4th Consumer Survey of WWW Users; University of Michigan Business School).

Jeżeli chodzi o preferencje odnośnie pośrednictwa firmy trzeciej, to wyglądają one w sposób następujący (oceny są w skali 1 do 5, im bliżej 5 tym większe zainteresowanie):



Wykres F Preferencje użytkowników odnośnie firm pośredniczących.(Źródło: 4th Consumer Survey of WWW Users; University of Michigan Business School).

Z dotychczas przeprowadzonych badań statystycznych nad wykorzystaniem Internetu wynika, że jest on wykorzystywany w sposób masowy przez osoby dobrze sytuowane, z których część dokonywała już zakupów za pośrednictwem Internetu. Fakty te zwiększają zainteresowanie przedsiębiorców komercyjnym wykorzystaniem Internetu, co oznacza konieczność szybkiego opracowania uniwersalnych metod bezpiecznych płatności. Wskazane jest także silniejsze zaangażowanie się w systemy płatności poprzez Internet poważnych instytucji finansowych, takich jak banki czy operatorzy kart płatniczych.

Gwałtownie rosnąca liczba użytkowników Internetu jest wynikiem atrakcyjności usług, jakie oferuje i łatwości korzystania z niego. Aby podłączyć się do Internetu z domowego komputera, wystarczy modem, odpowiednie oprogramowanie i konto u firmy, poprzez

którą łączymy się z Internetem. Wkrótce z Internetu korzystać będzie można także przez sieć telewizji kablowej, co umożliwi płynną transmisję informacji multimedialnej. Połączenie z Internetem oferują także od niedawna największe amerykańskie komercyjne sieci komputerowe: Compuserve, America Online, Prodigy, Delphi. Każda z tych sieci była uprzednio samowystarczalna. Ich podłączenie do Internetu jest świadectwem obecnego trendu do łączenia się wszystkich sieci w jedną globalną super-sieć.

1.3. HANDEL ELEKTRONICZNY

Angielski termin *electronic commerce*, czyli handel elektroniczny, oznacza niepapierową wymianę informacji handlowej za pośrednictwem EDI (Electronic Data Interchange- Elektronicznej Wymiany Danych), poczty elektronicznej, elektronicznych tablic ogłoszeniowych, EFT (Electronic Funds Transfer-Elektronicznej Wymiany Pieniędzy) i innych pokrewnych technologii.[7]

Handel elektroniczny znajduje najczęstsze zastosowanie w takich dziedzinach jak zaopatrzenie, finanse, podatki, transport; wszędzie tam, gdzie następuje wymiana informacji między przedsiębiorstwami. Papierowe dokumenty zastępuje się szybszym, pewniejszym, tańszym i bardziej wydajnym obiegiem w postaci elektronicznej.

Aczkolwiek handel elektroniczny służyć może do wymiany wszelkiego typu dokumentów, szczególnie istotna jest elektroniczna wymiana płatności. Systemy elektronicznej wymiany płatności są używane od lat 60. Początkowo działały w zamkniętych sieciach korporacyjnych, rozwiązania różnych producentów były wzajemnie niekompatybilne. Cechą takich dedykowanych systemów było ich zastosowanie do transakcji o dużej wartości. Andreas Crede z University of Sussex twierdzi[8], że w typowych transakcjach finansowych, jakkolwiek 85-90% wartości rozliczeń jest przetwarzane elektronicznie, to stanowi to tylko 5-10% całej liczby płatności. Reszta rozliczana jest ręcznie. Jako przyczyny tego stanu rzeczy podaje fakt, że elektroniczne systemy płatności opracowane były w zamkniętych sieciach i służyć

[7] Electronic Commerce Acquisition Program Management Office; http://www.gsa.gov/ecapmo/
[8] Electronic Commerce and the Banking Industry: The Requirements and Opportunities for New Payment Systems Using the Internet; http://www.usc.edu

miały raczej do rozliczania dużych, w znacznym stopniu międzynarodowych transakcji. Ich zastosowanie do transakcji o mniejszej wartości jest nieekonomiczne. Stopień skomplikowania, zabezpieczeń tych systemów i kontroli nad nimi sprawowanej, np. przez powołane do tego urzędy centralne, nie pozwala na ich zastosowanie do masowych płatności mniejszej wartości, jakie zaistnieją w momencie upowszechnienia się handlu przez Internet.

Dodatkowo z różnych powodów instytucjonalnych transakcje papierowe stanowią w dużym stopniu przyjętą normę, przez co nie poddają się zautomatyzowaniu. Pomimo gwałtownego rozwoju technik komunikacyjnych, dalej większość rozliczeń pomiędzy firmami dokonywana jest za pomocą czeków lub transferu telegraficznego.

Sprawa zautomatyzowania i przeniesienia płatności do postaci elektronicznej jest kluczowa dla obniżenia kosztów działalności. Według Konferencji ds. Handlu i Rozwoju ONZ[9] koszt papierowych rozliczeń w handlu międzynarodowym, ich sprawdzania, przesyłania, wprowadzania do wewnętrznych systemów informatycznych, przetwarzania, drukowania etc. wynosi do 10% wartości przesyłanych towarów. Łącznie w skali roku jest to ok. 400 miliardów USD zbędnych kosztów transakcyjnych.

Rozwiązaniem wydaje się być zastosowanie Internetu jako platformy rozliczania płatności, zarówno w ramach EDI, jak i powszechnego handlu elektronicznego. Systemy internetowe mogą być szczególnie dobrze przystosowane do taniego rozliczania niewielkich płatności, co może dać początek całkiem nowym możliwościom prowadzenia działalności gospodarczej.

1.4. KOMERCYJNE WYKORZYSTANIE INTERNETU

W przypadku Internetu pojęcie handel elektroniczny obejmuje szerokie spektrum usług. Najpopularniejsze to elektroniczne publikacje i reklama. Poprzez firmowy serwis WWW dystrybuowane są informacje o firmie i jej produktach, aktualnych cenach, wyprzedażach etc. Jest to najprostsza z form obecności w Internecie. Charakteryzuje się statycznością i stosunkowo małą funkcjonalnością. Bardziej rozbudowane serwisy

[9] United Nations Conference on Trade and Development; http://gatekeeper.unicc.org/unctad/

WWW umożliwiają pełniejszy kontakt z klientami. Mogą oni uzyskiwać wsparcie techniczne i dostarczać informacji zwrotnej (poprzez kwestionariusze). Najbardziej zaawansowane formy to jednoczesny marketing połączony ze sprzedażą. Przykładem mogą być elektroniczne sklepy, które nie tylko informują o oferowanych produktach, ale o ile to możliwe, umożliwiają zarówno ich dostarczenie, jak i płatność poprzez Internet. Często sklepy zgrupowane są razem tworząc elektroniczne centra handlowe (e-malls).

Do handlu poprzez Internet najlepiej nadają się dobra informacyjne, to jest takie, które można przełożyć na postać cyfrową i dostarczyć klientowi siecią. Do tej kategorii należą informacje tekstowe, programy, grafika, animacja, dźwięk. Przykładem mogą być elektroniczne gazety i specjalistyczne raporty. Przy obecnych, nie do końca dopracowanych jeszcze mechanizmach internetowego handlu, dobra informacyjne charakteryzują się dodatkowo mniejszym ryzykiem straty dla sprzedawców niż w przypadku dóbr fizycznych.

Internetowy handel niesie wiele korzyści przedsiębiorstwom. Umożliwi im bezpośredni dostęp do milionów potencjalnych konsumentów. Łatwe w użyciu bazy danych i katalogi umożliwiają łatwe skontaktowanie się klienta z obecną w Internecie firmą. Podobnie będzie się miała sytuacja z partnerami handlowymi i dostawcami. Firmy będą mogły ich wyszukiwać w prosty, szybki i tani sposób w Internecie. Dzięki użyciu on-line katalogów, zamówień i płatności, skrócony zostanie cykl zakupów. Zbędne staną się kosztowne, szybko dezaktualizujące się katalogi. Koszty własne firm zostaną obniżone poprzez dostęp do szerszego i bardziej konkurencyjnego rynku dostawców. Współpraca z kooperantami na wszystkich poziomach opracowywania i sprzedaży produktu skróci ich czas. Przy przyjmowaniu elektronicznych płatności łatwiejsze będzie zarządzanie płynnością. Klienci skorzystają ze zwiększonej konkurencyjności dostawców i sprzedawców, która obniży cenę i poprawi jakość zamawianych usług i towarów.

Internet jest idealnym medium dla małych przedsiębiorców, chcących sprzedawać stosunkowo tanie dobra informacyjne. Programiści mogą sprzedawać aplikacje, analitycy rynku finansowego-analizy, gospodynie domowe przepisy kucharskie etc. Praktycznie każdy może zostać sprzedawcą. Bariery wejścia na rynek są bardzo małe.

Oprócz dostępu do Internetu założyć należy konto u któregoś z dostawców systemu płatności. Za drobną opłatą pośredniczyć oni będą w sprzedaży danej informacji. Nie potrzeba mieć swojego serwera WWW. Wszystko odbywa się automatycznie. Autor dostarcza tylko informacje i pobiera wpływające pieniądze. Przy zastosowaniu elektronicznych pieniędzy nie potrzeba stosować kosztownych i skomplikowanych procedur autoryzacji kart kredytowych.

Tacy mikro-sprzedawcy generować będą olbrzymią ilość mikro-płatności, wartości pojedynczych centów lub dolarów. Będzie to na tyle tanie dla kupujących, by mogli oni sobie na to pozwolić, a jednocześnie duża liczba kupujących da satysfakcjonujący dochód i zachętę mikro-sprzedawcom. Poszukując materiałów do badań, naukowiec chętnie wyda drobną sumę pieniędzy na przygotowane przez kogoś dobrej jakości opracowania, a następnie wynik swojej pracy będzie mógł sam umieścić w Internecie i sprzedawać. Dla powodzenia tej unikalnej idei mikro-płatności i mikro-sprzedawców ważne jest opracowanie takich mechanizmów płatności, które dobrze by je wspierały. Muszą być proste w użyciu i mieć znikome koszty transakcyjne.

1.5. INTERNET W BANKOWOŚCI

Internet zaczyna być także coraz powszechniej wykorzystywany w bankowości. Pod koniec maja 1996 Reuter podał[10], że w USA jedna na sto transakcji bankowych osób fizycznych zlecona została poprzez telefon lub komputer. Analitycy oceniają, że w roku 1998 będzie to 14% operacji bankowych. Przewiduje się, że w ciągu kilkunastu lat nieopłacalne okaże się posiadanie rozbudowanej sieci lokalnych oddziałów. Większość transakcji dokonywana będzie zdalnie z domu czy biura.

Do tej pory najczęściej używane w elektronicznej bankowości są systemy home-banking, gdzie klient używając specjalnej aplikacji łączy się z bankiem poprzez modem. Jest to wygodne dla klienta, który może dokonywać operacji bankowych 24 godziny na dobę. Dla banków oznacza to nowych klientów i zmniejszone koszty działalności poprzez redukcję obciążenia lokalnych oddziałów i sprawniejszy obieg dokumentów.

[10] Gazeta Wyborcza, Biuro-Komputer nr 21, 21 maja 1996, str. 10

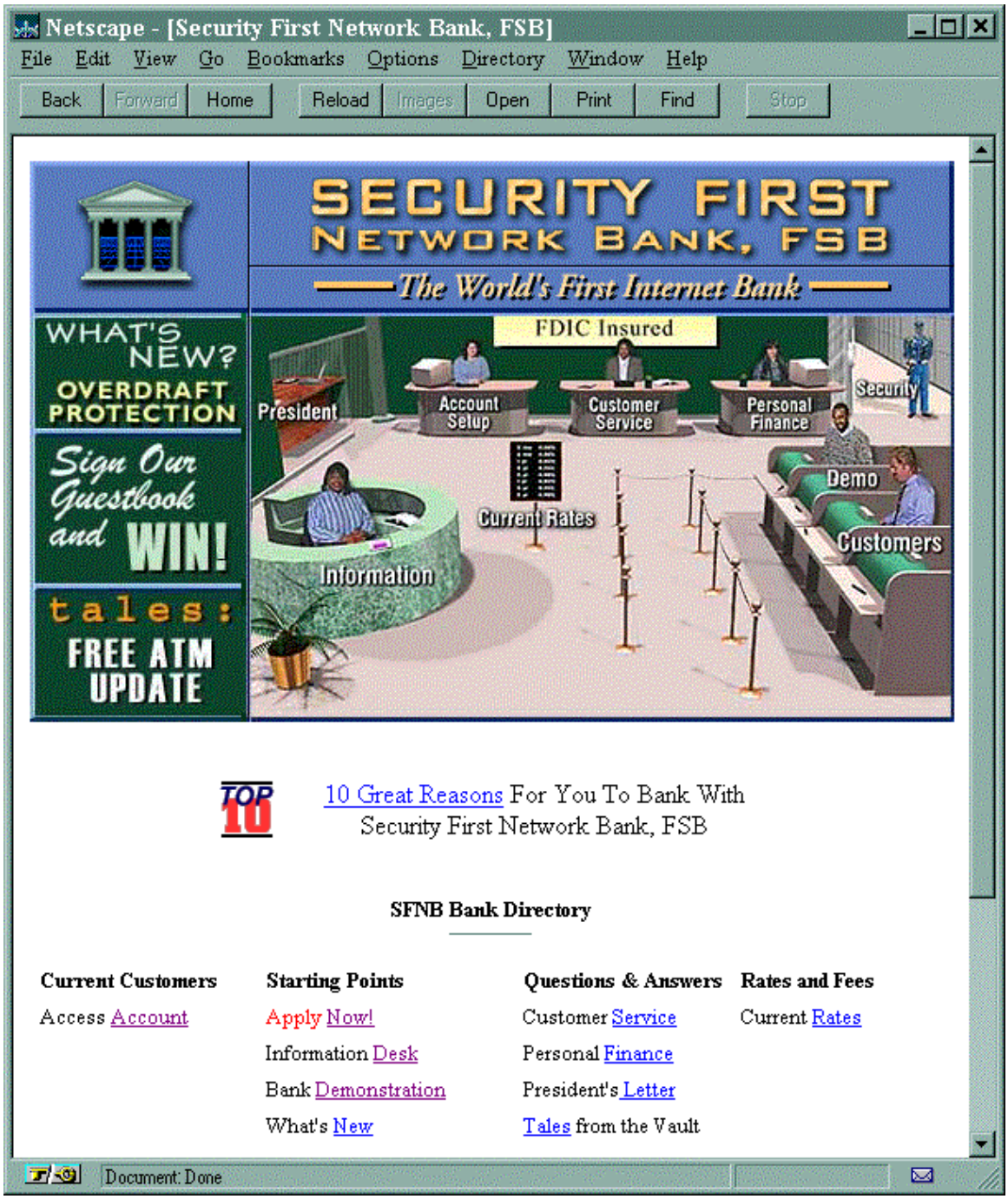
Do home-banking mogą też być używane popularne pakiety do prowadzenia domowych finansów, takie jak Microsoft Money czy Quicken firmy Intuit. Pakiety te umożliwiają modemowe połączenia z wspierającymi to rozwiązanie bankami, co integruje domowe rozliczenia z możliwością aktualizacji danych i zdalnego dokonywania transakcji.

Przyszłością bankowości wydaje się jednak być Internet-banking, czyli oferowanie usług bankowych poprzez Internet. Sposób ten ma duże zalety w porównaniu z tradycyjnym home-banking. Nie wymagane jest żadne specjalistyczne oprogramowanie. Klient posiadać musi jedynie przeglądarkę WWW. Całość oprogramowania spoczywa na serwerze WWW banku. W przypadku zmiany działania oprogramowania czy dodania nowych opcji, klient od razu ma do nich dostęp. W podejściu tradycyjnym musiałby za każdym razem zaopatrywać się w uaktualnioną wersję programu.

Lawinowo rośnie liczba osób używających Internetu. Wiedząc, jak poruszać się po WWW, są oni w stanie instynktownie korzystać z usług wirtualnych banków.

Przykładem banku operującego głównie w Internecie jest Security First Network Bank[11].

[11] http://www.sfnb.com/



Rysunek A Strona tytułowa serwisu WWW Security First Network Bank.

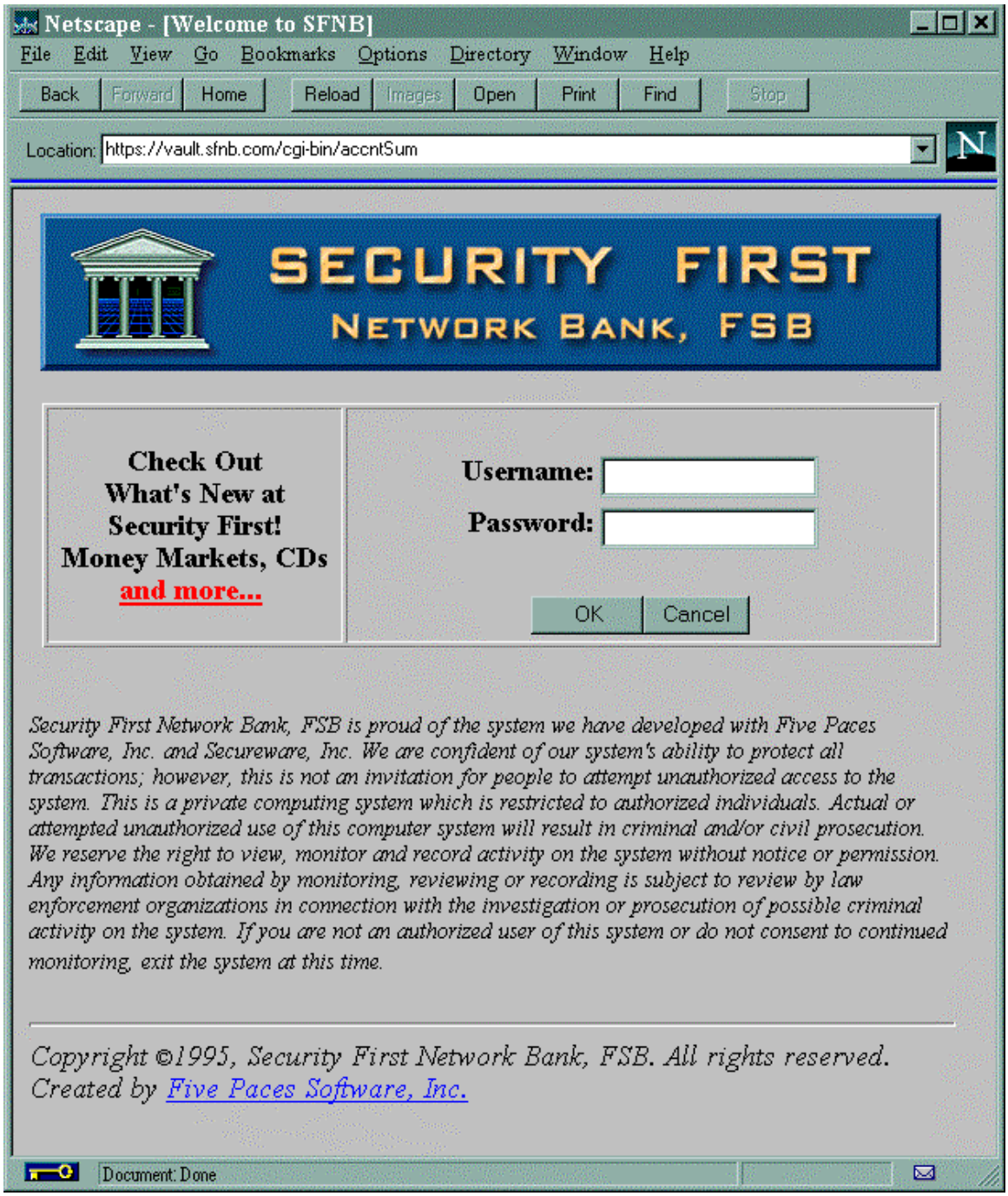
Klikając na poszczególnych obszarach strony przedstawiającej lobby banku mamy do dyspozycji różne usługi, takie jak np. zakładanie konta, informacja czy operacje bankowe.

Security First Network Bank oferuje obecnie rachunki bieżące, certyfikaty depozytowe i konta rynków pieniężnych (money markets accounts). Wkrótce oferować ma karty kredytowe, konta dla firm, doradztwo finansowe, usługi brokerskie i inne usługi

bankowe. Z dostępności banku w Internecie wynika np. to, że otwarty jest 24 godziny na dobę i potencjalnie korzystać mogą z niego klienci na całym świecie (chwilowo z powodów formalnych rachunki otwierać w nim mogą jedynie obywatele USA). Specjalnie opracowane zabezpieczenia gwarantują pełne bezpieczeństwo transakcji. System działa na zmodyfikowanym do celów bankowych systemie operacyjnym opracowanym przez SecureWare[12]. Dodatkową gwarancją bezpieczeństwa dla klientów jest to, że podobnie jak w tradycyjnych bankach są oni ubezpieczeni do wysokości 100 000 USD przez FDIC (Federal Deposit Insurance Corporation) -rządową organizację ubezpieczającą banki, które muszą stosować się do jej zaleceń w dziedzinie bezpieczeństwa bankowego.

Klienci posiadający konto w Security First Network Bank logują się najpierw do systemu, podając swój identyfikator i hasło, a następnie dokonują operacji bankowych.

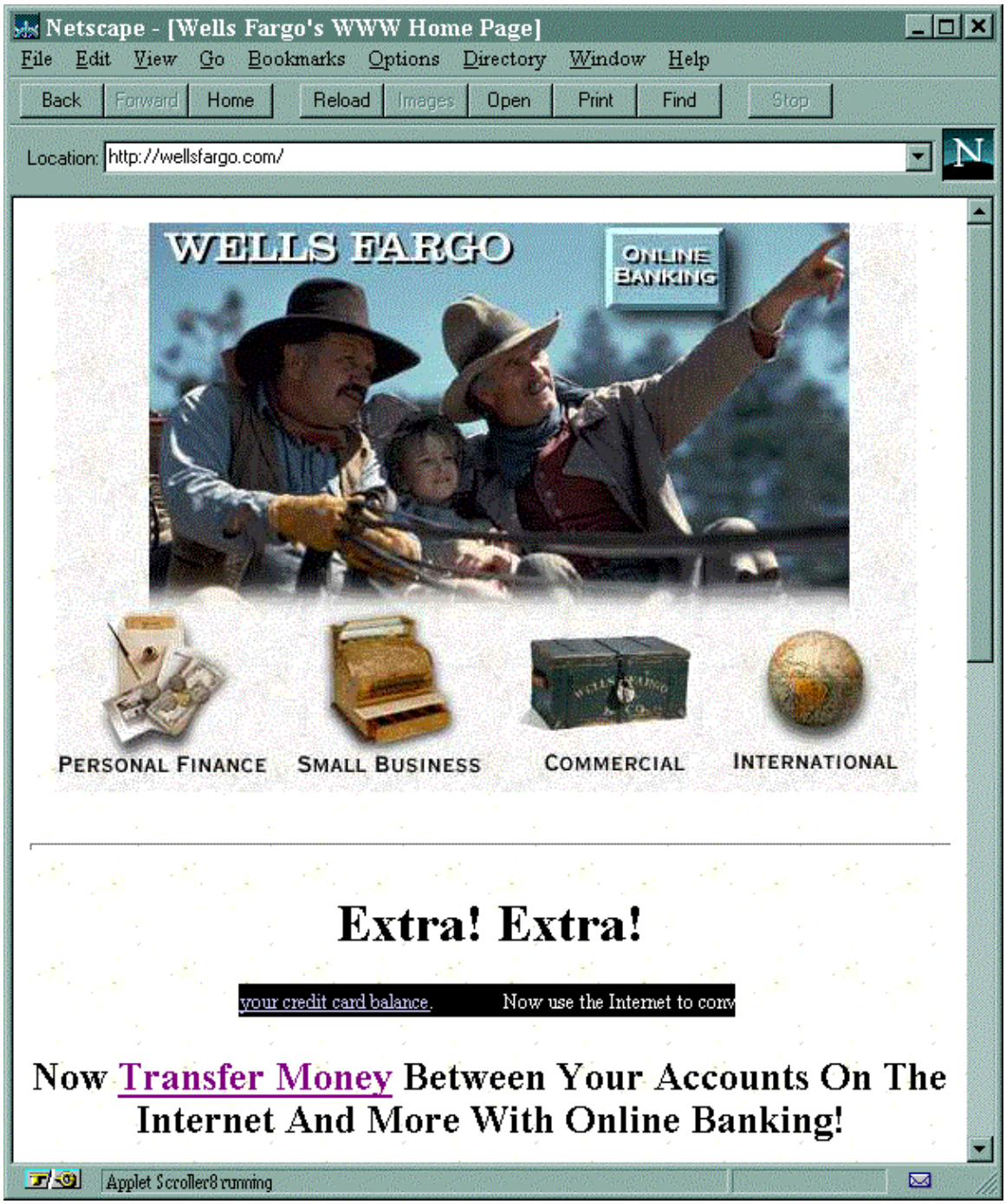
[12] http://www.secureware.com



Rysunek B Logowanie się do systemu Security First Network Bank za pomocą przeglądarki WWW.

Mogą np. przeglądać historię dokonywanych przez siebie operacji, płacić rachunki, drukować raporty z przychodów i wydatków. Wszystko co klientowi potrzebne, by korzystać z usług tego banku, to konto w nim, które może dostać on-line, dostęp do Internetu i przeglądarka WWW.

Innym bankiem udostępniającym home-banking poprzez Internet jest amerykański bank Wells Fargo[13].



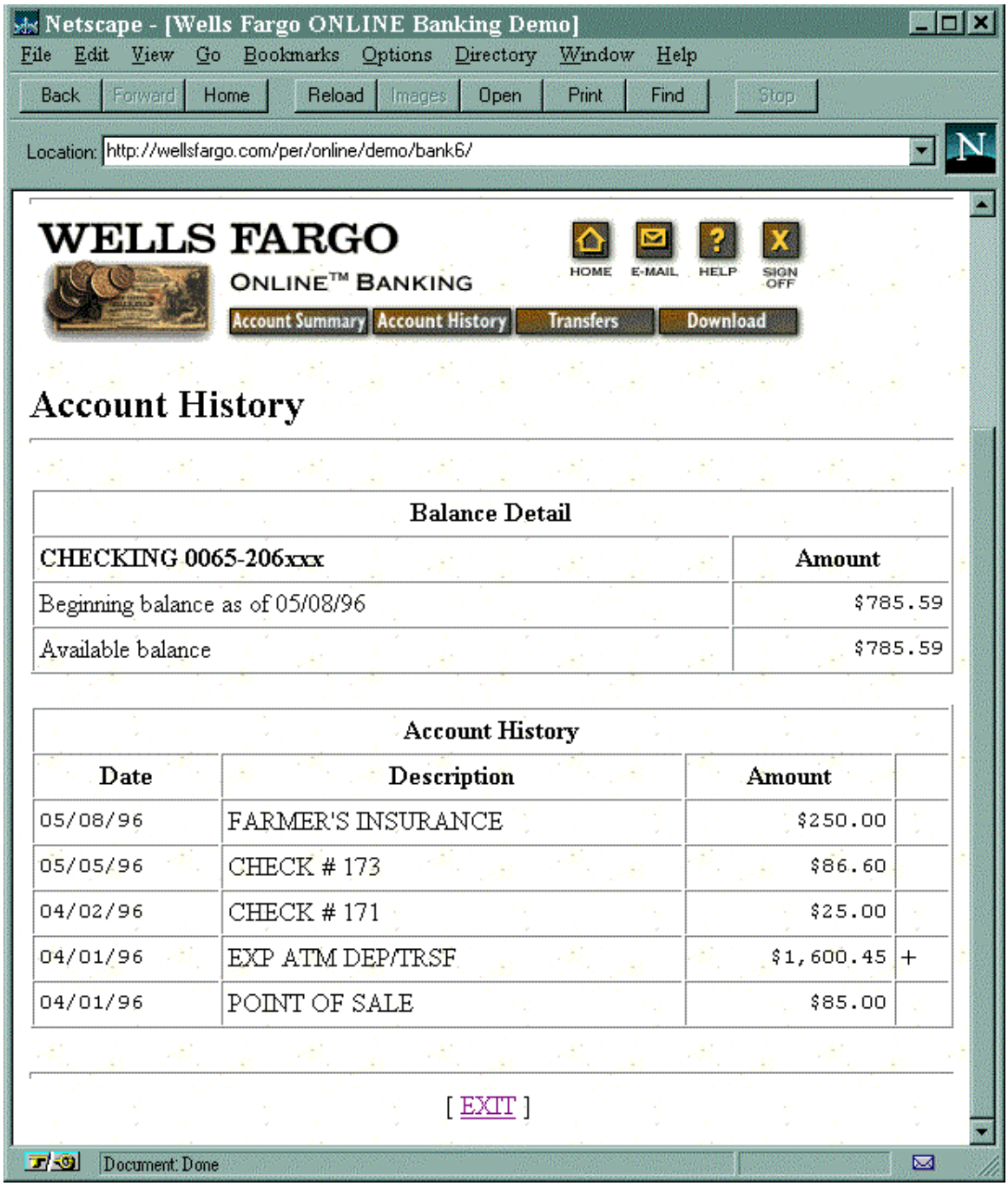
Rysunek C Strona tytułowa WWW banku Wells Fargo.

Poprzez Internet daje on swoim klientom dostęp do ich kont i możliwość ściągnięcia danych w formacie najpopularniejszych pakietów zarządzania osobistymi finansami.

[13] http://wellsfargo.com/

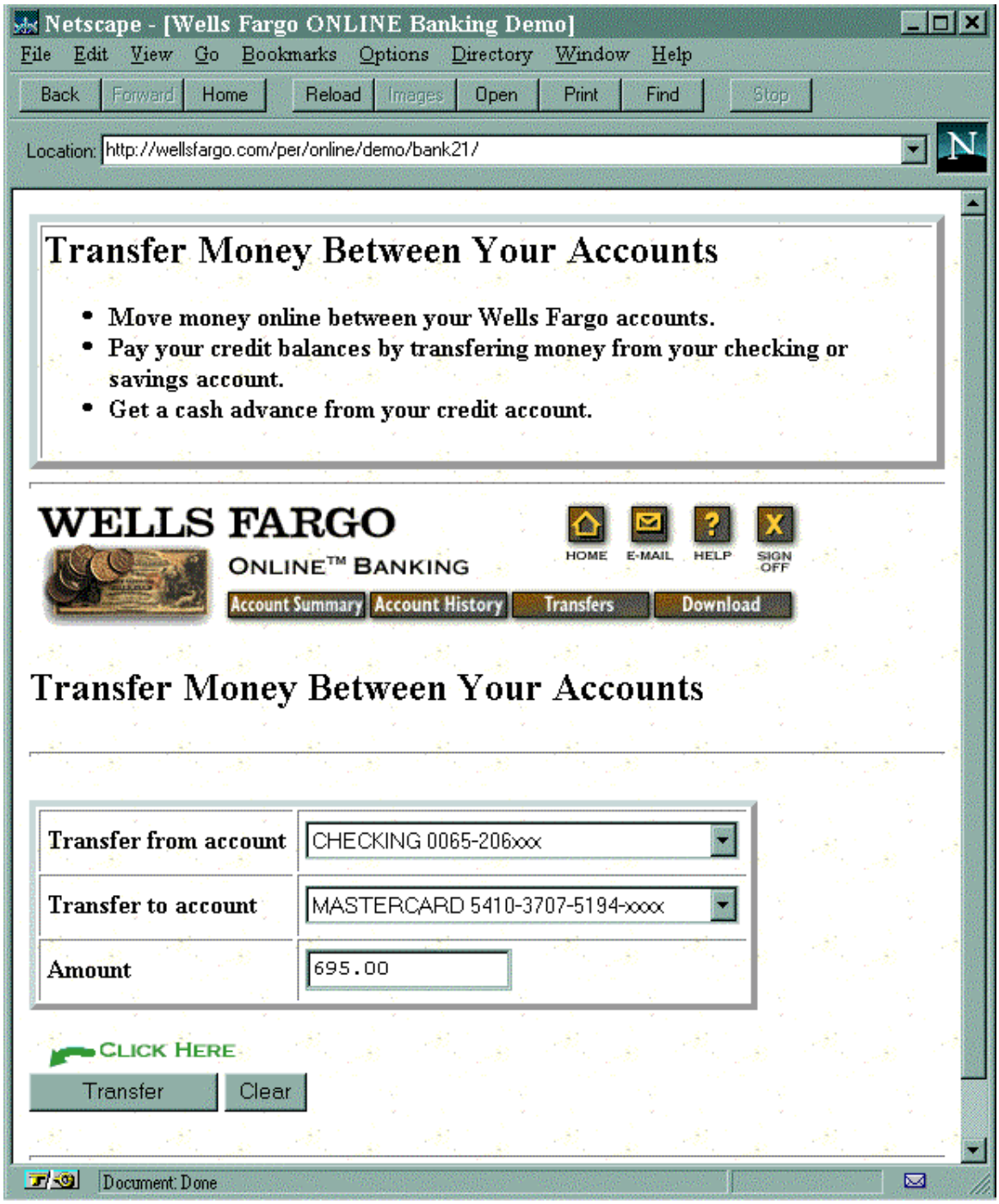
Rysunek D Okno WWW Wells Fargo pokazujące posiadane rachunki bankowe.

Można wybrać interesujące nas konto i obejrzeć dokładną historię przeprowadzanych na nim operacji.



Rysunek E Okno WWW Wells Fargo przedstawiające historię operacji na danym koncie.

Łatwo dokonuje się przelewów między posiadanymi kontami.



Rysunek F Okno WWW Wells Fargo, dokonywanie przelewu z konta na konto.

Bankowość przez Internet (Internet banking) wydaje się być kierunkiem rozwoju bankowości. Jej zalety w postaci łatwości użycia i powszechnej dostępności mogą spowodować, że stanie się preferowaną przez klientów formą kontaktu z bankiem.

1.6. JAK WYGLĄDA DOKONYWANIE ZAKUPÓW POPRZEZ INTERNET

Zakupy poprzez Internet realizowane są z reguły w technologii World Wide Web, tj. sklep zbudowany jest ze stron globalnej pajęczyny i klient dokonuje zakupów posługując się przeglądarką WWW. Najpierw, zwykle poprzez któryś z internetowych katalogów, znajdujemy sklep oferujący interesujące nas towary.

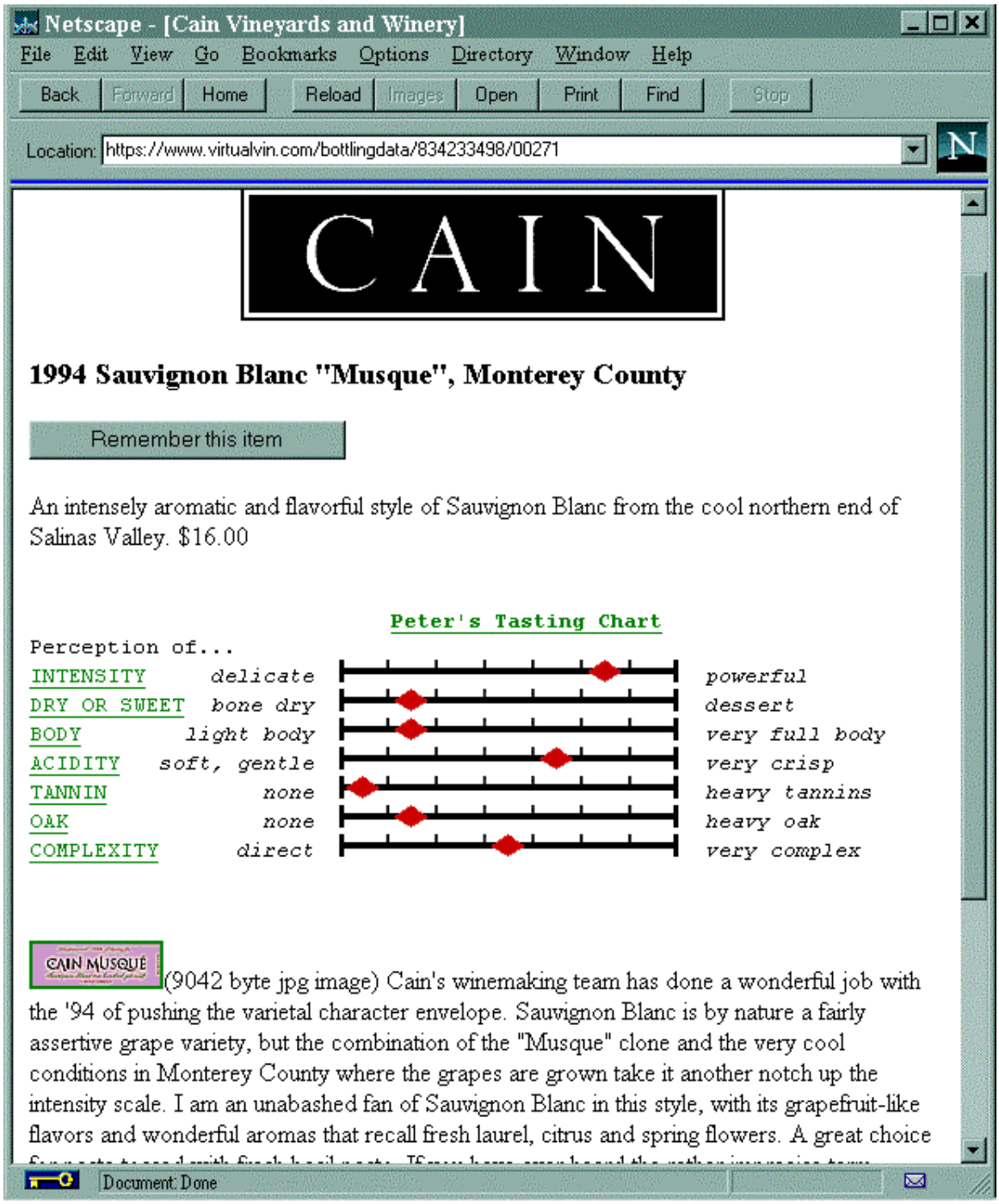
W naszym przykładzie będzie to sklep z ekskluzywnymi winami.

Rysunek G Strona tytułowa przykładowego sklepu internetowego.

Przeglądamy oferowaną listę towarów i posługując się myszką wybieramy ten, który nas interesuje. Ponieważ jest to hipertekst, przeniesieni zostaniemy do kolejnego okna.

Rysunek H Katalog sprzedawanych produktów w przykładowym elektronicznym sklepie.

Możemy dostać bardziej dokładny opis wybranej przez nas pozycji i „włożyć” ją do naszego elektronicznego „koszyka”, czyli sprawić, by serwer zapamiętał nasz wybór.

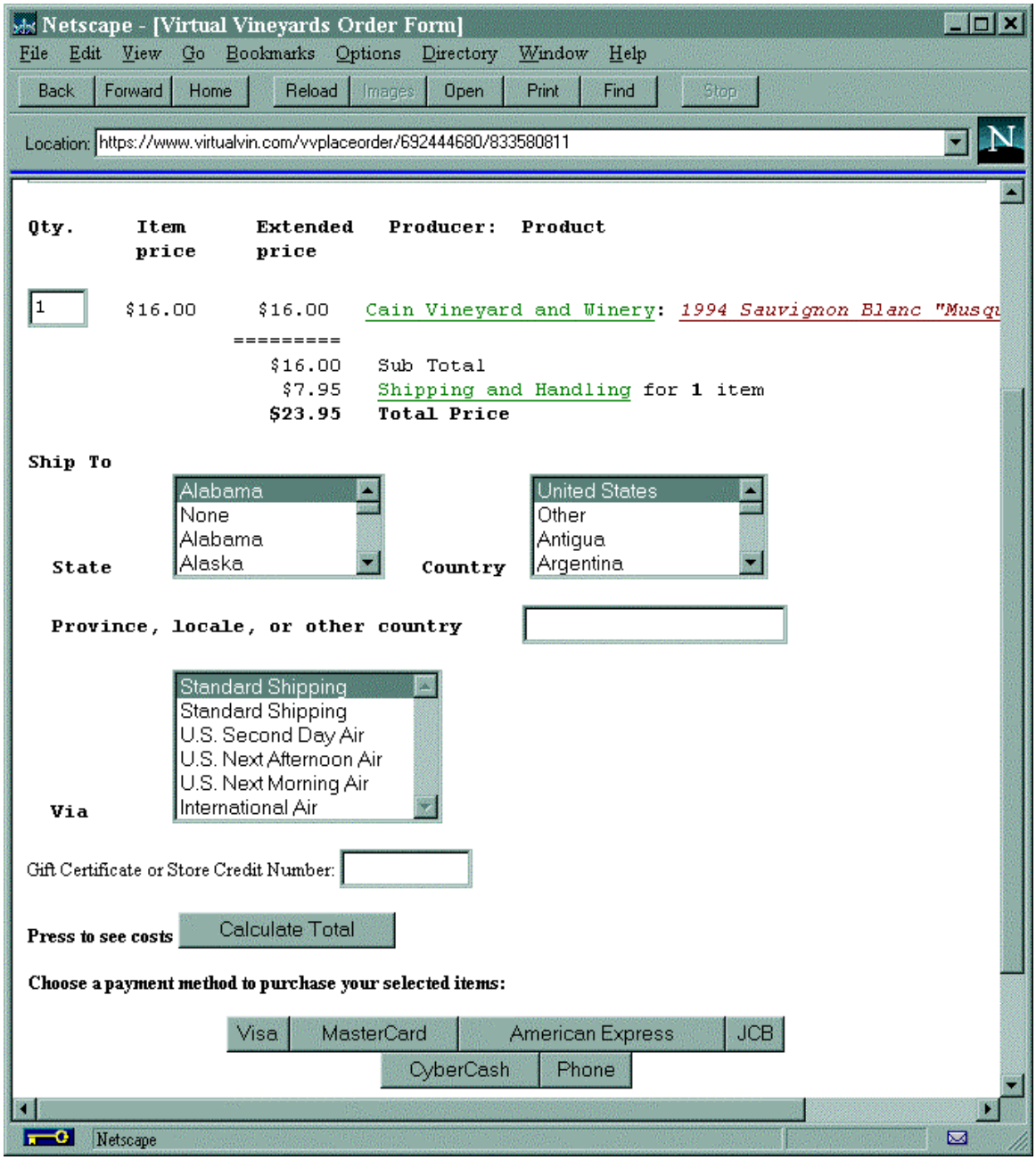


Rysunek I Szczegółowe informacje o produkcie w przykładowym elektronicznym sklepie.

Na koniec przechodzimy do ekranu, na którym możemy wybrać ilość zamawianego produktu, podać adres, na który chcemy go wysłać i wybrać metodę płatności. Nasz

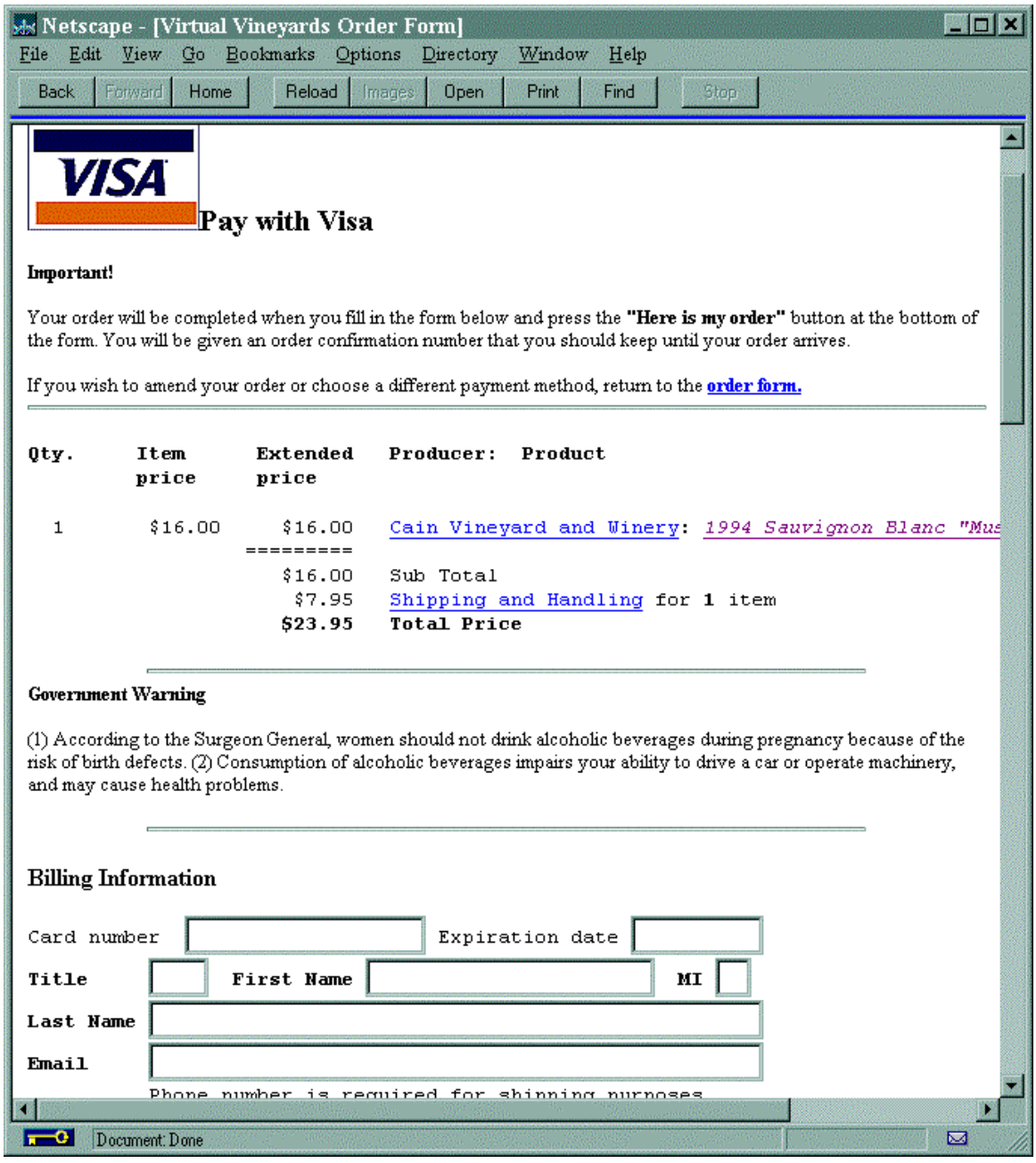
przykładowy sklep oferuje płatność przez telefon, różne karty kredytowe w trybie „Secure Netscape” i CyberCash. Dane te wpisujemy do okienek dialogowych i wybieramy z list wyboru. Komputer poda wartość zamówienia, razem z opłatami za dostawę, pakowanie i podatek.

Załóżmy, że chcemy zapłacić przy użyciu karty kredytowej Visa.



Rysunek J Wybór sposobu zapłaty w przykładowym elektronicznym sklepie.

Wpisujemy dane karty kredytowej i dokładny adres, na który ma zostać wysłana przesyłka.



Rysunek K Dokonywanie płatności w przykładowym elektronicznym sklepie.

Detale naszego zamówienia, razem z informacjami o sposobie płatności, zostaną przesłane do sprzedawcy. Po uzyskaniu autoryzacji karty kredytowej u jej wystawcy sprzedawca wyśle pocztą elektroniczną potwierdzenie zamówienia oraz wyekspediuje pocztą zamówiony towar.

2. INTERNETOWE SYSTEMY P□ATNO□CI

2.1. WPROWADZENIE

W obecnej chwili dostępnych jest wiele konkurencyjnych technologii umożliwiających dokonywanie płatności poprzez Internet. Część z nich jest dopiero w fazie testów. Systemy te podlegają ciągłym modyfikacjom, pojawiają się nowe rozwiązania. Aktualne systemy płatności elektronicznych przez Internet oparte są na wykorzystaniu istniejących protokołów składowych TCP/IP. Są to przede wszystkim: poczta elektroniczna (SMTP/RFC822/MIME), telnet, finger, FTP i globalna pajęczyna WWW (HTTP).

Największym problemem płatności przez Internet jest zapewnienie bezpiecznej transmisji danych, ich integralności i autentyfikacji[14] komunikujących się stron. Standardowo Internet nie zapewnia żadnej z tych cech. Informacja w drodze od nadawcy do odbiorcy wędruje w postaci nie zaszyfrowanej przez wiele komputerów pośredniczących. Każdy, kto ma fizyczny dostęp do którejś z tych maszyn, może przechwycić przesyłane przez nią dane (sniffing). Dlatego nie powinno się transmitować przez Internet w postaci odkrytej numerów kart kredytowych, kont bankowych, haseł etc.

Eliminuje to zastosowanie potencjalnie najprostszej z metod płatności, polegającej na przesyłaniu pocztą elektroniczną lub przeglądarką WWW numeru karty kredytowej. Po serii wypadków przechwycenia poufnych informacji przez komputerowych włamywaczy, metody tej praktycznie się już nie stosuje. Odpowiednie ekrany ostrzegawcze zostały wbudowane w przeglądarki WWW. W normalnym trybie pracy informują one, że przesyłanie danych siecią nie gwarantuje ich poufności.

Firmy proponujące poszczególne systemy płatności stosują dodatkowe mechanizmy dla zapewnienia bezpieczeństwa transakcji. Zwykle opierają się one na kryptografii. Możliwe jest jednak ominięcie tego problemu i posługiwanie się Internetem tylko do

[14] słowo *autentyfikacja* używane będzie w znaczeniu weryfikacji tożsamości, tj. możliwości stwierdzenia, czy dany użytkownik naprawdę jest tym, za kogo się podaje

wybrania produktu/usługi i przekazania zamówienia, podczas gdy płatność realizowana jest w sposób tradycyjny, tj. podając przez telefon numer karty kredytowej, wysyłając faksem lub pocztą czek czy przekaz pieniężny. Jest to najprostszy i historycznie pierwszy ze sposobów internetowych płatności. Aczkolwiek daje bezpieczeństwo (przyjmuje się, że poczta i telefon są bezpiecznymi mediami), to nie wykorzystuje w pełni potencjału Internetu. Sposób ten jest niewygodny dla kupującego, naraża go na dodatkowe koszty i nie sprzyja ważnym dla sprzedawców, impulsywnym zakupom. Nie można go uważać za pełnowartościową metodę płatności. Sposób ten jest jednak ciągle stosowany, najczęściej w połączeniu z innymi systemami. Pozostanie zapewne w użyciu do czasu opracowania stuprocentowo pewnych i przyjętych jako standard metod płatności przez sieć.

Druga kategoria proponowanych systemów oferuje płatność w pełni za pośrednictwem Internetu. Także bazuje na posiadanych już przez klientów środkach płatniczych, takich jak czeki (system NetCheque) czy karty kredytowe. Rozwiązania opierające się na karcie kredytowej stosują szyfrowanie przesyłanych danych (CyberCash, Netscape) albo metody zastępcze, które nie wymuszają przesyłania poufnych informacji przez sieć (First Virtual).

Oddzielną kategorią rozwiązań są elektroniczne pieniądze (e-cash), proponowane przez DigiCash i NetCash, oraz związane z nimi karty chipowe (Mondex i pokrewne).

2.2. KARTY KREDYTOWE

Dla zastosowania w płatnościach Internetowych niezbędne jest opracowanie metody bezpiecznej transmisji numeru karty, daty jej ważności i innych informacji zwykle wymaganych do dokonania transakcji. Karty kredytowe są najbardziej popularną metodą płatności internetowych. Do zalet należy ich popularność i prostota użycia. Posługuje się nimi miliony klientów. Płacąc kartą kupujący jest ubezpieczony przez jej wystawcę na wypadek oszustwa sprzedawcy.

Karta kredytowa ma także wady:

- posługiwanie się nią jest drogie: często są opłaty minimalne, przy transakcjach niedużej wartości (typowych dla Internetu) opłaty mogą przewyższyć wartość

transakcji. Eliminuje to ich zastosowanie do mikro-płatności, które są siłą napędową internetowego handlu;

- sprzedający musi być akredytowany przez wystawcę karty, co jest możliwe dopiero po spełnieniu całego szeregu warunków;
- płatności kartą kredytową nie są w pełni anonimowe;
- karta kredytowa nie może być stosowana do prywatnych przepływów pomiędzy konsumentami;
- występują limity kredytowe i inne ograniczenia narzucane przez emitentów;
- karta kredytowa nie jest dostępna dla każdego, występując o nią trzeba mieć dobrą historię kredytową;
- nie każdy lubi i chce używać kart kredytowych, u wielu wywołujących kosztowny nałóg wydawania więcej niż sobie można na to pozwolić.

2.2.1. CyberCash

Powstała w 1994 roku amerykańska firma CyberCash[15] jest jednym z liderów wśród firm dostarczających rozwiązań dla bezpiecznego stosowania kart kredytowych w internetowych płatnościach. Oferowany przez firmę system składa się z 3 zasadniczych części:

- elektronicznego portfela (electronic wallet)- darmowego programu instalowanego przez klienta na swoim komputerze;
- darmowego modułu sprzedawcy, instalowanego przez sprzedawcę na swoim serwerze;
- modułu pośredniczącego między kupującym a sprzedającym obsługiwanego przez CyberCash, zapewnia on autoryzację transakcji w czasie rzeczywistym.

Obecnie elektroniczny portfel CyberCash umożliwia płatności tylko przy użyciu kart kredytowych. Następne wersje mają mieć także możliwość płacenia kartami

[15] http://www.cybercash.com

debetowymi, elektronicznymi pieniędzmi i regulowania tzw. mikro-płatności, co umożliwi zakupy o zbyt małej wartości, by rozliczać je za pomocą kart kredytowych.

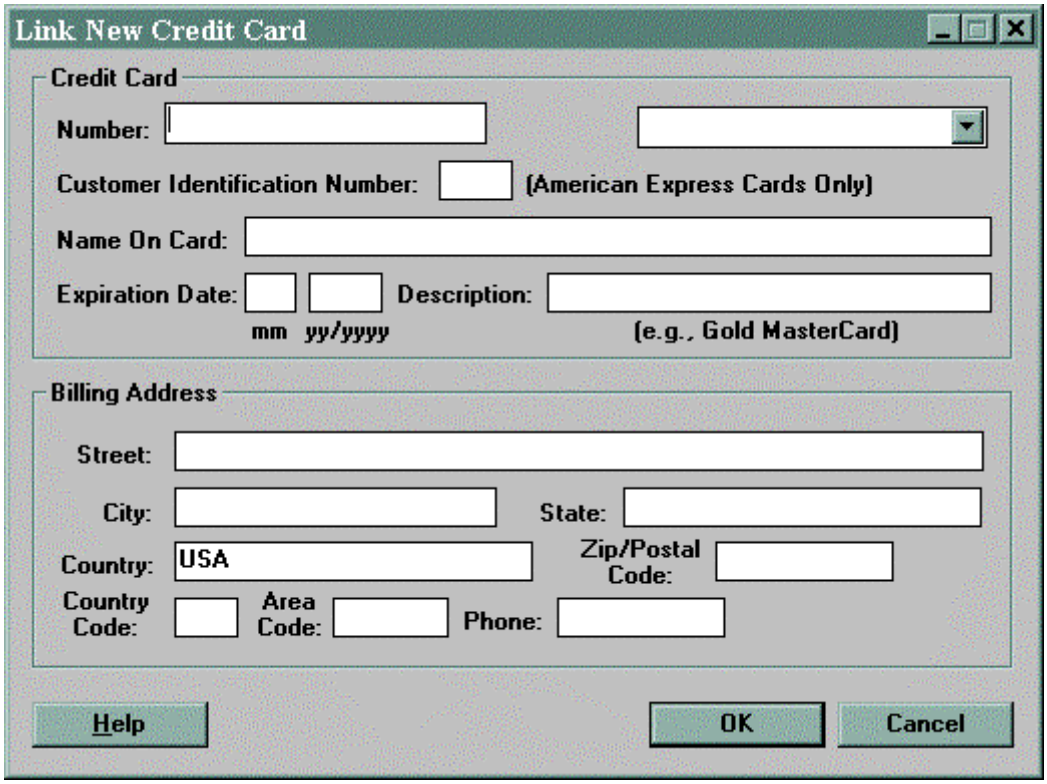
Do posługiwania się systemem CyberCash niezbędna jest aplikacja klienta, nazywana elektronicznym portfelem CyberCash. Można ją bezpłatnie uzyskać w Internecie[16] z serwera firmy CyberCash w wersji na Windows i na Macintosha. Oprogramowanie jest bardzo proste w użyciu. Po instalacji program poprosi nas o zarejestrowanie się, co stworzy nasz elektroniczny portfel. Podajemy wymyślony przez nas identyfikator i wpisujemy nasz adres poczty elektronicznej. Identyfikatorem może być nazwisko, pseudonim lub dowolny ciąg znaków, ważne, by jednoznacznie identyfikował właściciela portfela.

Rysunek L Rejestracja nowego użytkownika elektronicznego portfela CyberCash.

Dla zabezpieczenia portfela podajemy wymyślone przez nas hasło (6-20 znaków), po czym wygenerowany zostanie unikalny kod bezpieczeństwa użytkownika. Portfel ma wbudowane moduły komunikacji sieciowej poprzez Internet. Korzystając z nich połączy się siecią z centralą firmy. Jeżeli wybrany przez nas identyfikator jest już używany, zaproponowany zostanie nowy, który możemy zaakceptować lub zmodyfikować. Dostęp do portfela mają tylko osoby znające identyfikator i hasło.

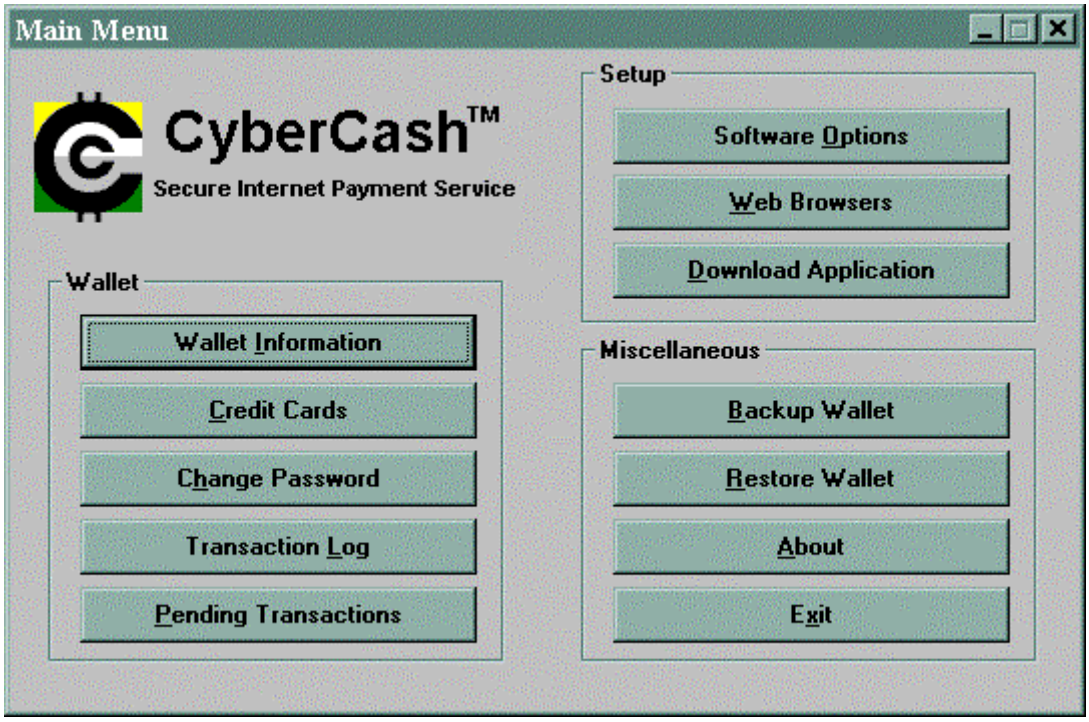
[16] http://ftp.cybercash.com/WinCyber.html

Chcąc używać portfela musimy skojarzyć go z przynajmniej jedną kartą kredytową. Do wyboru mamy 6 najpopularniejszych rodzajów kart, w tym Visa, MasterCard, American Express. Jeśli posiadamy kilka kart, należy wpisać je wszystkie, tak byśmy mogli płacić każdą z nich. Wypełnione przez nas dane karty kredytowej są szyfrowane i transmitowane do CyberCash, który przeprowadza ich weryfikację przy pomocy wystawcy karty. Przy zmianie hasła wszystkie dane portfela będą zaszyfrowane na nowo.



Rysunek M Kojarzenie elektronicznego portfela CyberCash z kartą kredytową.

Następnie pokaże się menu główne programu.



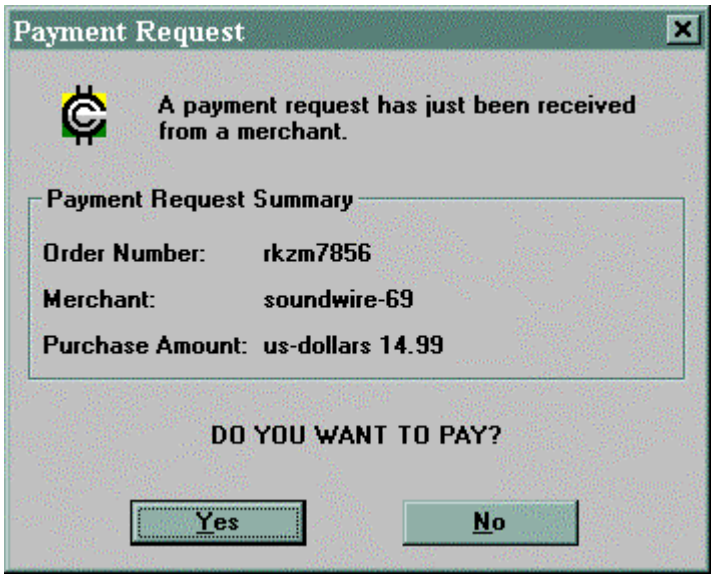
Rysunek N Główne menu programu CyberCash Wallet.

W lewym panelu (Wallet) możemy zmienić nasz adres poczty elektronicznej (Wallet Information), dodać i usunąć karty kredytowe (Credit Cards), zmienić hasło (Change Password), przejrzeć historię transakcji (Transaction Log), zobaczyć które z transakcji oczekują na zakończenie (Pending Transactions).

W prawym górnym panelu (Setup) możemy zmienić opcje działania programu (Software Options), takie jak ewentualny adres HTTP Proxy serwera, numer portu etc. Można też ręcznie skojarzyć portfel z używaną przeglądarką WWW (Web Browsers), a także uzyskać najnowszą wersję oprogramowania z serwera CyberCash (Download Software). Aktualizacja oprogramowania może zostać przeprowadzona automatycznie, jeżeli podczas transakcji system sprzedawcy wykryje, że posługujemy się starą wersją portfela.

W panelu „Różne" (Miscellaneous) możemy wybrać dodatkowe operacje, takie jak zrobienie kopii danych z portfela na dysk/dyskietkę (Backup Wallet), odtworzenie ich (Restore Wallet), informacja o programie (About) i zakończenie pracy programu (Exit).

Płatności za pośrednictwem CyberCash dokonuje się poprzez przeglądarkę WWW, portfel współpracuje z prawie wszystkimi ich rodzajami. Kupujący ogląda ofertę sprzedawcy i wybiera to, co chciałby kupić. Następnie naciska przycisk „zapłać" na stronie WWW sprzedającego, co uruchamia automatycznie elektroniczny portfel CyberCash, rezydujący na komputerze klienta. Pokazuje się okienko z informacjami o zakupie, takimi jak identyfikator sprzedawcy, numer zakupu, suma do zapłacenia i ewentualnie lista towarów czy usług, za które płacimy.



Rysunek O Okienko zapłaty wygenerowane przez system CyberCash.

Wybieramy którąś z kart kredytowych, które uprzednio skojarzyliśmy z portfelem i naciskamy przycisk „zapłać". Zaszyfrowana informacja zostanie wysłana do sprzedawcy, który usuwa informację o szczegółach zamówienia, dodaje do niego swój elektroniczny podpis i przesyła w postaci zaszyfrowanej do serwera CyberCash. CyberCash odszyfrowuje transmisję w specjalnym sprzętowym czytniku, reformatuje ją i przesyła dedykowanymi liniami (nie Internetem) do banku sprzedawcy. Bank uzyskuje autoryzację zakupu przy pomocy danej karty u jej wystawcy i przesyła kod zgody lub odmowy zapłaty z powrotem do CyberCash, który ponownie szyfruje informacje (o tym, czy płatność została autoryzowana) i przesyła ją do sprzedawcy, który z kolei przekazuje klientowi potwierdzenie zakupu (lub komunikat o niezaakceptowaniu przez bank karty) i zrealizuje dostawę zamówionego towaru/usługi. Cała operacja, po zainicjowaniu przez klienta płatności, trwa około 15-20 sekund.

Informacja o karcie kredytowej przechowywana jest wyłącznie (w postaci zaszyfrowanej) na komputerze klienta. CyberCash przechowuje informacje o karcie kredytowej tylko w formie umożliwiającej pamiętanie, do kogo dana karta jest przypisana. Informacje o tym, jakie zakupy robi klient posługując się daną kartą, nie są rejestrowane. Także sprzedawca nie widzi parametrów karty kredytowej kupującego.

Sprzedawca chcący posługiwać się systemem CyberCash do przyjmowania należności musi skontaktować się z firmą i podpisać umowę licencyjną. Musi także wystąpić do swojego banku o pozwolenie na przyjmowanie kart kredytowych (jeżeli jeszcze go nie ma), zaznaczając, że zamierza przyjmować transakcje internetowe za pośrednictwem systemu CyberCash. Sprzedawca konieczne oprogramowanie uzyskuje bezpłatnie z serwera CyberCash.

Obecnie CyberCash rozdał ponad 400 000 swoich elektronicznych portfeli. Firma współpracuje z 80% amerykańskich banków. Rozwiązanie CyberCash jest kompatybilne z podobnymi elektronicznymi portfelami firm Compuserve i Checkfree. CyberCash jest także jedyną firmą amerykańską mającą pozwolenie na zastosowanie i eksport 768-bitowego algorytmu szyfrowania RSA.

System płatniczy CyberCash jest działającym rozwiązaniem, z którego mogą korzystać klienci chcący i mogący płacić kartami kredytowymi (a wkrótce i innymi kartami płatniczymi oraz elektronicznymi pieniędzmi). Daje klientowi dużą łatwość dokonywania zakupów. Obsługa elektronicznego portfela nie sprawia żadnego problemu. Nie trzeba za każdym razem wpisywać wszystkich danych karty kredytowej, zachęca to do bardziej impulsywnych zakupów. Klient ma zawsze dostęp do historii swoich zakupów, prowadzonej przez elektroniczny portfel. System jest sprawdzony i bezpieczny, działa u wielu sprzedawców, zaakceptowany został przez banki. Zaawansowane mechanizmy szyfrowania sprawiają, że transakcje są bezpieczne niezależnie od rodzaju użytej przeglądarki WWW.

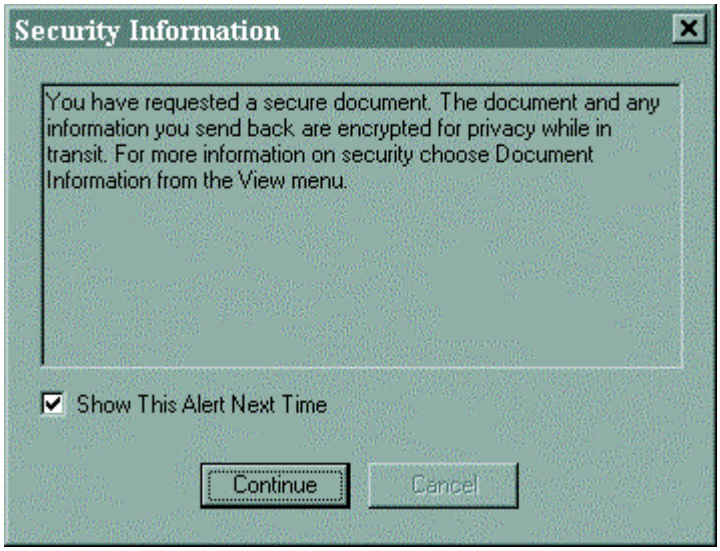
2.2.2. Secure Netscape

Główną zaletą tego systemu jest łatwość posługiwania się nim. Nie potrzeba zakładać dodatkowych kont bankowych. Transakcja jest podobna do tej, której powszechnie dokonują klienci korzystając z zakupów telefonicznych czy pocztowych. Nie trzeba instalować żadnego specjalnego oprogramowania, tak jak ma to miejsce np. w systemie CyberCash. Do transakcji wymagana jest jedynie już posiadana karta kredytowa i przeglądarka WWW korzystająca z mechanizmu SSL, opracowanego przez firmę Netscape. SSL umożliwia bezpieczne przekazywanie danych, takich jak parametry karty kredytowej, przez przeglądarkę WWW.

Robiąc zakupy wybieramy towary, za które chcemy zapłacić, a następnie wpisujemy dane karty do formularza zakupu. Są one bezpiecznie transmitowane do sprzedawcy.

Połączenie zabezpieczone mechanizmem SSL wyświetlane jest odpowiednio na przeglądarce. Dookoła okna dokumentu pojawia się niebieska ramka, ikona przerwanego klucza w dolnym lewym rogu zmienia się w cały klucz, w opcji „Document Info” z menu „View” można uzyskać niektóre informacje z certyfikatu SSL serwera, co zapewnia jego weryfikację. Dodatkowo przeglądarka Netscape Navigator często pokazuje różnego rodzaju okna dialogowe w sytuacji, gdy wchodzimy do obszaru zabezpieczonego, wychodzimy z niego, wysyłamy nie zaszyfrowane informacje etc.

O połączeniu z serwisem zabezpieczonym mechanizmem SSL informuje następujące okienko:



Rysunek P Rozpoczęcie pracy w systemie SSL przy użyciu przeglądarki Netscape Navigator.

Szyfrowanie zabezpiecza przed podsłuchiwaczami przesyłaną informację, nie stanowi jednak gwarancji tożsamości nadawcy. Ktokolwiek zna numer karty kredytowej i inne podstawowe informacje, może podszyć się pod właściciela i złożyć fałszywe zamówienie, dokładnie tak jak przez telefon. Jakkolwiek ubezpieczenie chroni w pewnym stopniu konsumenta przed takimi nadużyciami, jest to jednak zawsze kłopotliwe. Dodatkowo wysokie koszta transakcyjne autoryzacji karty powodują, że sposób ten nie nadaje się do najpopularniejszych w Internecie mikro-płatności.

2.2.3. First Virtual

First Virtual Holdings utworzony został w początkach 1994 roku. Jest jedną z czołowych firm zaangażowanych w handel elektroniczny. Swój system elektronicznych płatności internetowych uruchomił 15 października 1994 roku.

Główną cechą charakteryzującą rozwiązanie zaproponowane przez First Virtual jest unikalne podejście do kwestii bezpieczeństwa. Nie są używane żadne metody kryptograficzne. Poufne informacje nie muszą być i nigdy nie są przesyłane Internetem.

Transakcje handlowe pomiędzy sprzedającym a kupującym zawiera się najczęściej posługując się przeglądarką WWW, chociaż równie dobrze można użyć poczty elektronicznej, FTP czy IRC.

Aby zostać użytkownikiem systemu, czyli nabyć prawa do robienia zakupów posługując się systemem płatności First Virtual, należy posiadać dwie rzeczy:

- kartę kredytową systemu Visa lub Master Card;
- internetowy adres poczty elektronicznej (adres musi być prywatny, tj. nie dzielony z żadną inna osobą).

Posługując się przeglądarką WWW wypełniamy elektroniczny formularz zawierający nasze nazwisko, adres zamieszkania i poczty elektronicznej (jeśli nie mamy przeglądarki, formularz wypełnić można także przy użyciu poczty elektronicznej lub telnetując się na specjalne konto). Niezbędne w procesie rejestracji dane odnośnie karty kredytowej przekazujemy telefonicznie na bezpłatny numer First Virtual. Usługa ta jest automatyczna, czyli posługując się aparatem tonowym obejdziemy się bez pomocy personelu firmy.

W wyniku rejestracji First Virtual przesyła nam pocztą elektroniczną specjalny numer identyfikacyjny klienta, nazywany przez firmę Virtual PIN. Numer ten zastępuje od tej pory numer karty kredytowej i umożliwia zakupy poprzez Internet. Rejestracja kosztuje 2 USD. Nie ma żadnych dodatkowych opłat związanych z wysokością lub częstością zakupów.

Gdy znajdziemy interesujący nas towar, po wybraniu go sprzedawca poprosi nas o podanie numeru Virtual PIN, ewentualnie także o informacje dodatkowe, takie jak adres odbiorcy.

Rysunek Q Płatność w systemie First Virtual.

Sprzedający przekazuje pocztą elektroniczną informacje o planowanej sprzedaży do centrali First Virtual, która sprawdzając załączony w poczcie Virtual PIN, odszukuje w swojej bazie danych skojarzony z danym klientem adres poczty elektronicznej i przesyła mu wiadomość z prośbą o potwierdzenie zamiaru dokonania zakupu.

Kupujący może na takie zapytanie odpowiedzieć na jeden z trzech sposobów:

- „yes” oznaczające: „tak, chcę to kupić i zamierzam za to zapłacić”;
- „no” oznaczające: „nie, nie chcę tego kupić”;
- „fraud” oznaczające „oszustwo, ktoś się za mnie podaje”.

Równie prosto przebiega rejestracja osób chcących zostać sprzedawcami w systemie elektronicznych płatności First Virtual. Potrzeba tylko:

- wypełnić elektroniczny formularz;
- posiadać konto w banku akceptującym depozyty bezpośrednie (w amerykańskim systemie ACH);
- przesłać czek na 10 USD tytułem opłaty rejestracyjnej.

Ogłaszając swoją ofertę, sprzedający może skorzystać z pośrednictwa First Virtual i wykupić uczestnictwo w programie InfoHaus, kojarzącym kupujących i sprzedających. Dotychczas najczęściej oferowane są produkty informacyjne, tj. dające się przesłać siecią, czyli programy komputerowe, grafika, muzyka, tekst, filmy, informacje etc. Większość sprzedawców stosuje dodatkowo politykę „spróbuj, zanim kupisz”, co pozwala na bezpłatne wgranie produktu lub jego części dla celów testowych.

Bezpieczeństwo opracowanego przez First Virtual sposobu transakcji finansowych przez Internet opiera się na fakcie, że poprzez Internet nigdy nie jest przekazywany, zarówno w postaci odkrytej jak i szyfrowanej, ani numer karty kredytowej, ani żadne inne poufne informacje. Przekazywany jest jedynie Virtual PIN, którego atrakcyjność dla złodzieja stosującego technikę „sniffing” (podglądania płynących siecią danych) jest znikoma, jako że nie można go wykorzystać poza Internetem, a w Internecie wymagane jest dodatkowe potwierdzenie za pośrednictwem poczty elektronicznej. Gdy użytkownik podejrzewa, że ktoś przechwycił jego Virtual PIN, np. otrzymując prośbę z First Virtual o potwierdzenie zakupów, których nie dokonał, powinien odpowiedzieć na to „fraud”, co spowoduje natychmiastowe i permanentne anulowanie Virtual PIN. Dla złamania zabezpieczenia, jakie daje Virtual PIN i dokonania oszustwa, złodziej musiałby nie tylko w jakiś sposób przechwycić sekretny numer Virtual PIN, ale także uzyskać dostęp do konta i skrzynki pocztowej klienta, monitorować jego przychodzącą pocztę i podszyć się pod niego w momencie wymaganego przez First Virtual potwierdzenia zakupu.

Atrakcyjność oferty First Virtual polega na tym, że konsekwencją nieprzesyłania przez sieć żadnych poufnych informacji jest to, iż klient nie musi posiadać żadnego specjalnego oprogramowania szyfrującego czy obsługującego transakcje. Jedyne co jest wymagane, to własne konto poczty elektronicznej. Prostota i wygoda tego rozwiązania stanowi o przewadze tej metody nad schematami płatności kartami kredytowymi opartymi na kryptografii.

System jest także anonimowy. Virtual PIN nie zawiera żadnych informacji osobistych. Sprzedający zna tylko imię i nazwisko kupującego, takie jakie podał on na formularzu rejestracyjnym. Może to być pseudonim lub nazwa firmy. W ten sposób kupujący wie, że informacja o tym, co i kiedy kupuje, nie jest dostępna osobom postronnym.

2.3. ELEKTRONICZNE PIENIĄDZE

Metody płatności kartami kredytowymi, aczkolwiek z wielu powodów atrakcyjne dla kupujących, nie dają się zastosować w każdej sytuacji. Karty kredytowe nie gwarantują pełnej anonimowości transakcji, nie umożliwiają prywatnych przepływów gotówki pomiędzy konsumentami. Ze względu na wysokie koszty transakcyjne nie nadają się do mikro-płatności. Minimalną wartością transakcji dla karty kredytowej jest 15-20 USD.

Internet jest szansą dla całej masy drobnych sprzedawców oferujących tanie usługi i informacje. Potrzebują oni innego, taniego mechanizmu internetowych płatności. Takim rewolucyjnym mechanizmem są elektroniczne pieniądze (e-cash, cybercash). Wydają się być naturalnym krokiem w gwałtownie postępującej ewolucji Internetu. Potencjalnie jest to perfekcyjny środek wymiany. Daje możliwość błyskawicznego regulowania zobowiązań przy znikomych kosztach transakcyjnych. W sposób idealny realizuje jedną z funkcji pieniądza: środka wymiany.

Pieniądze elektroniczne, w zależności od zastosowanej technologii, mogą być:

- anonimowe, czyli takie, które nie ujawniają tożsamości posiadacza (tak jak gotówka);
- identyfikujące, ujawniające tożsamość kupującego;

- hybrydowe: pieniądze mogą być anonimowe względem sprzedającego, ale jawne dla banku lub anonimowe w całości, lecz pozwalające na odtworzenie ich obiegu bez ujawniania tożsamości właściciela.

Elektroniczne pieniądze możliwe są dzięki zastosowaniu zaawansowanej kryptografii, a konkretnie metod: klucza publicznego, elektronicznego podpisu, ślepego podpisu (blind signature).

Idealne elektroniczne pieniądze powinny posiadać wszystkie zalety gotówki i inne pożądane cechy, które niesie zastosowanie nowoczesnej technologii:

1. Bezpieczeństwo. Raz użyte elektroniczne pieniądze nie mogą być wydane ponownie, nie powinno być możliwości ich podrobienia.
2. Łatwość użycia. Skomplikowane szczegóły implementacji elektronicznych pieniędzy (kryptografia, sprzęt) powinny być przezroczyste dla użytkownika, tak by mógł się nimi łatwo posługiwać.
3. Przenośność. Powinny być możliwe do użycia niezależnie od miejsca. Powinno się je móc łatwo transportować (nosić w kieszeni, np. w postaci karty chipowej), ich użycie nie powinno być ograniczone do określonych systemów komputerowych.
4. Możliwość wykorzystania off-line, tak jak gotówki. Do przekazywania pieniędzy nie powinna być wymagana weryfikacja instytucji pośredniczącej.
5. Bezpośredniość. Powinna być możliwość bezpośredniego przekazywania elektronicznych pieniędzy innej osobie prywatnej, nie będącej zarejestrowanym sprzedawcą.
6. Podzielność. Jednostka elektronicznych pieniędzy powinna być podzielna na mniejsze jednostki, tak by umożliwić dokonywanie dużej ilości zakupów o małej wartości.
7. Nieograniczony czas ważności. Powinno się je móc przechowywać w nieskończoność, dopóki nie zostaną zniszczone, zgubione lub ich wystawca nie zbankrutuje.
8. Szeroka akceptowalność. Elektroniczne pieniądze emitowane przez wielu różnych emitentów powinny być wymienialne.
9. Anonimowość. Płatność za pośrednictwem elektronicznych pieniędzy powinna być anonimowa. Nikt nie może wiedzieć na co, kiedy i ile wydaje dany konsument.

10. Wydajność. Elektroniczne pieniądze muszą mieć znikome koszty transakcyjne, systemy sprzedawców i pośredników muszą być w stanie sprostać wymaganiom technicznym i sprawnościowym.

Liderem w promowaniu idei elektronicznych pieniędzy jest holenderska firma DigiCash[17].

2.3.1. DigiCash

Założycielem i dyrektorem DigiCash jest dr David Chaum, autor pionierskich opracowań teoretycznych z dziedziny elektronicznych pieniędzy.

Firma oferuje różne technologie elektronicznych płatności: karty chipowe, rozwiązania czysto programistyczne lub mieszane. Promowane przez DigiCash elektroniczne pieniądze to rozwiązanie czysto softwarowe. Ma ono umożliwić dokonywanie płatności z dowolnego komputera, za pośrednictwem poczty elektronicznej lub innych usług Internetu. Firma zaangażowana jest także w przedsięwzięcie Komisji Europejskiej *Project CAFE*[18], mające na celu opracowanie elektronicznego portfela, przy pomocy którego będzie można używać elektronicznych pieniędzy poza Internetem.

Elektroniczne pieniądze DigiCash są obecnie w fazie testów. W ramach projektu rozpoczętego w październiku 1994 roku firma wypuściła testowy pieniądz elektroniczny- *Cyberbuck* (cybernetyczny dolar). W ciągu 12 miesięcy swój udział zarejestrowało prawie 30 000 osób, z których każda otrzymała 100 cyberdolarów, zdeponowanych w First Digital Bank- komputerowym banku DigiCash. Aczkolwiek nie mogą być one wymienione na prawdziwe pieniądze, to można się nimi posługiwać do zakupu produktów i usług w uczestniczących w programie setkach sklepów, które też mają swoje konta w First Digital Bank.

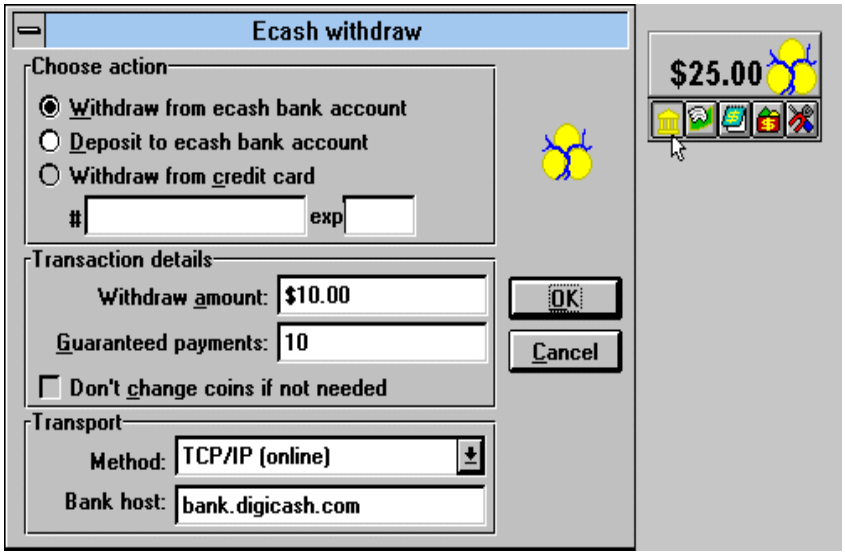
[17] http://www.digicash.nl
[18] http://www.digicash.com/products/projects/cafe.html

Wynikiem udanego programu testowego było licencjonowanie przez DigiCash technologii elektronicznych pieniędzy bankom i innym instytucjom finansowym zainteresowanym wypuszczaniem własnych elektronicznych pieniędzy. Pierwszym bankiem, który rozpoczął emisję prawdziwych elektronicznych pieniędzy, wymiennych na amerykańskie dolary, był Mark Twain Bank[19] z St. Louis, USA.

Proces założenia konta (World Currency Access) i uzyskania możliwości posługiwania się elektronicznymi pieniędzmi jest bardzo prosty. Na serwerze WWW banku wypełniamy elektroniczny formularz (federalne przepisy USA wymagają dodatkowego przesłania wypełnionych, podpisanych formularzy pocztą). Następnie przesyłamy czek lub przelew bankowy na konto Mark Twain Bank, który z kolei przesyła na podany przez nas adres poczty elektronicznej numer konta, hasło i instrukcje umożliwiające instalację specjalnego oprogramowania elektronicznego portfela (Ecash Software). Działa ono na najpopularniejszych platformach systemowych: Windows, Macintosh, UNIX. Dzięki zastosowaniu graficznego interfejsu użytkownika jest także bardzo proste w użyciu.

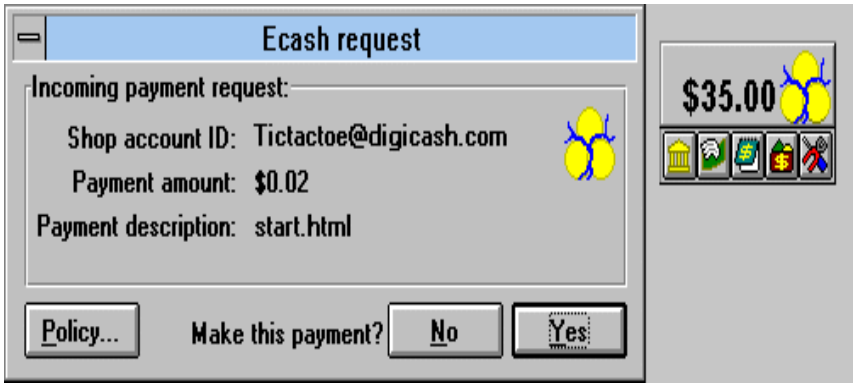
[19] http://www.marktwain.com/

Obecnie nie ma żadnych opłat za założenie konta czy minimalnej wymaganej sumy depozytu. Po przelaniu określonej sumy pieniędzy na konto World Currency Access możemy zażądać (faxem, telefonicznie lub poprzez email), aby określona suma została przełożona na elektroniczne pieniądze (Ecash Mint). Następnie przy użyciu elektronicznego portfela możemy zdeponować na naszym twardym dysku część lub całość pieniędzy. Będą one służyły do robienia zakupów.



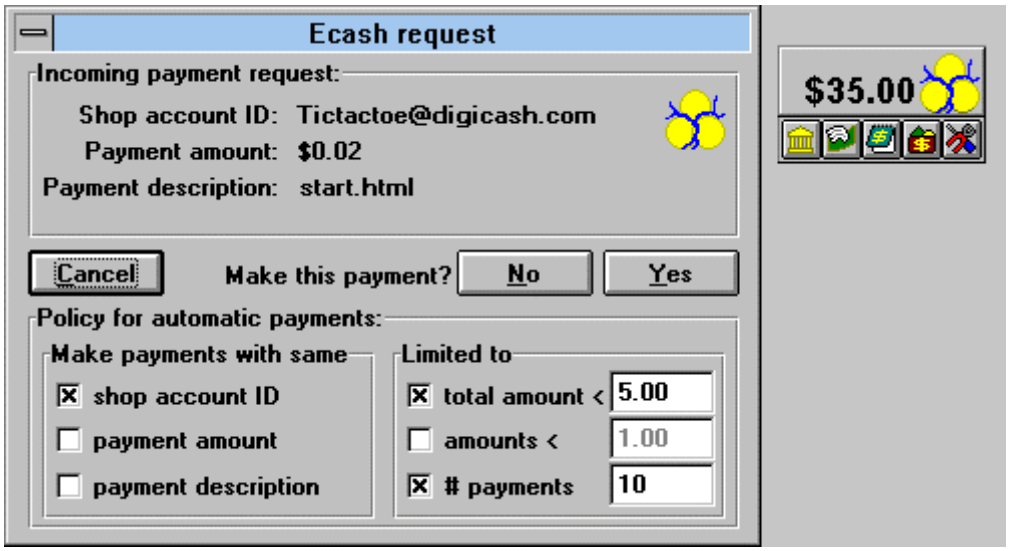
Rysunek R Przelanie pieniędzy z konta na twardy dysk (Źródło: DigiCash, ecash client ver 2.1 dla Windows).

Program jest zintegrowany z przeglądarką WWW i oprogramowaniem sprzedawcy, które generuje żądanie zapłaty. Elektroniczny portfel uaktywnia się automatycznie, gdy wybierzemy przycisk „zapłać" w serwisie WWW sprzedawcy.



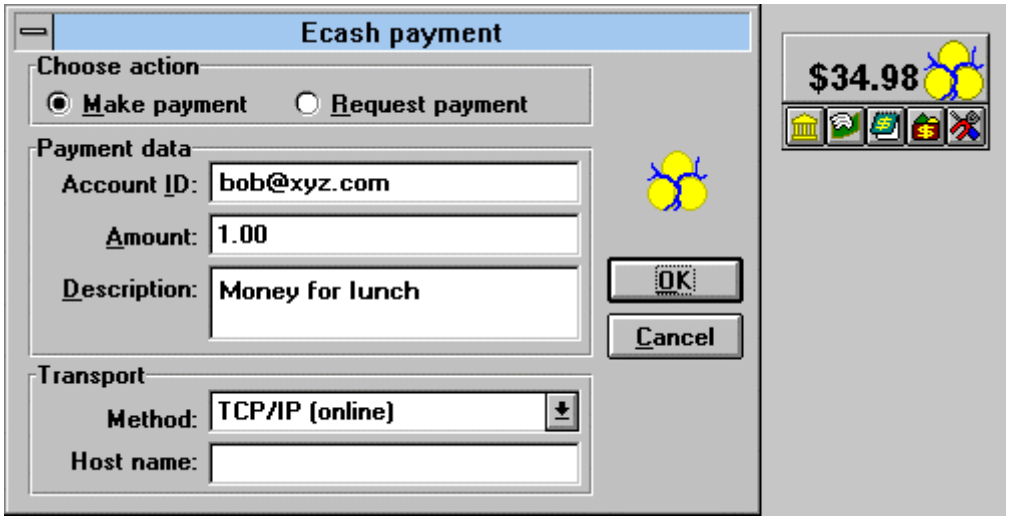
Rysunek S Żądanie zapłaty (Źródło: DigiCash, ecash client ver 2.1 dla Windows).

W przypadku regularnych zakupów o określonej sumie lub u określonych sprzedawców, system daje możliwość zdefiniowania sytuacji, gdy zapłata ma być uiszczana automatycznie.



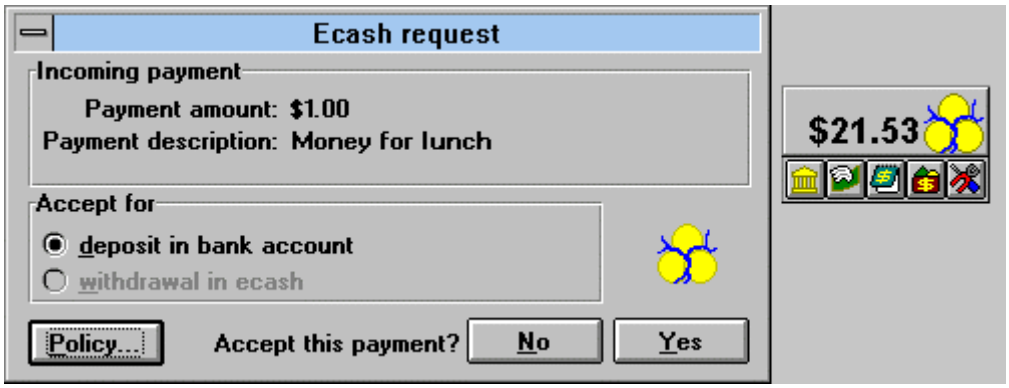
Rysunek T Ustalanie mechanizmu automatycznych płatności (Źródło: DigiCash, ecash client ver 2.1 dla Windows).

Pieniądze możemy także przesłać bezpośrednio osobom prywatnym (o ile posługują się one systemem Ecash). Podobnie możemy zażądać od kogoś zapłaty. Przyciskamy odpowiednią ikonkę programu i wypełniamy niezbędne parametry.



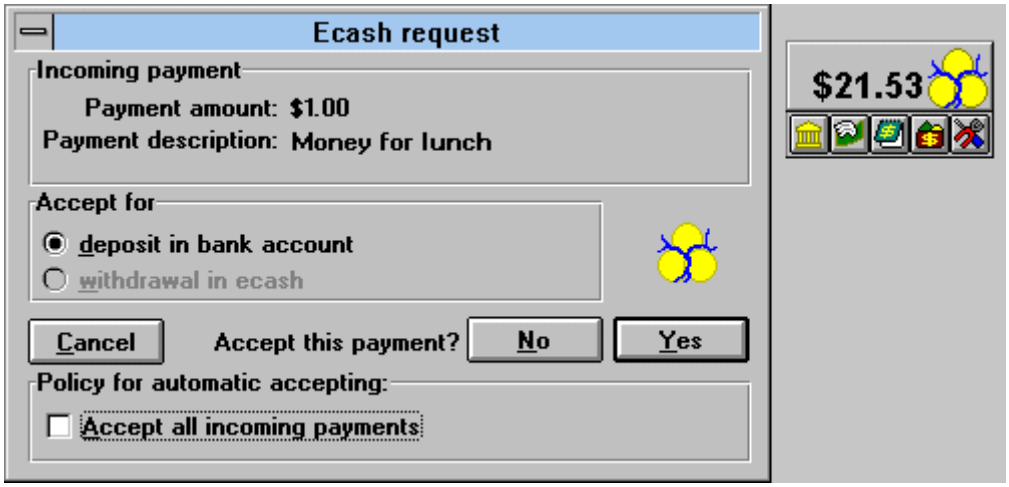
Rysunek U Dokonywanie płatności na rzecz osoby trzeciej. (Źródło: DigiCash, ecash client ver 2.1 dla Windows).

Wybrana przez nas osoba zostanie poinformowana o nadchodzących pieniądzach przez odpowiedni ekran, który daje możliwość przyjęcia lub odrzucenia przelewu.



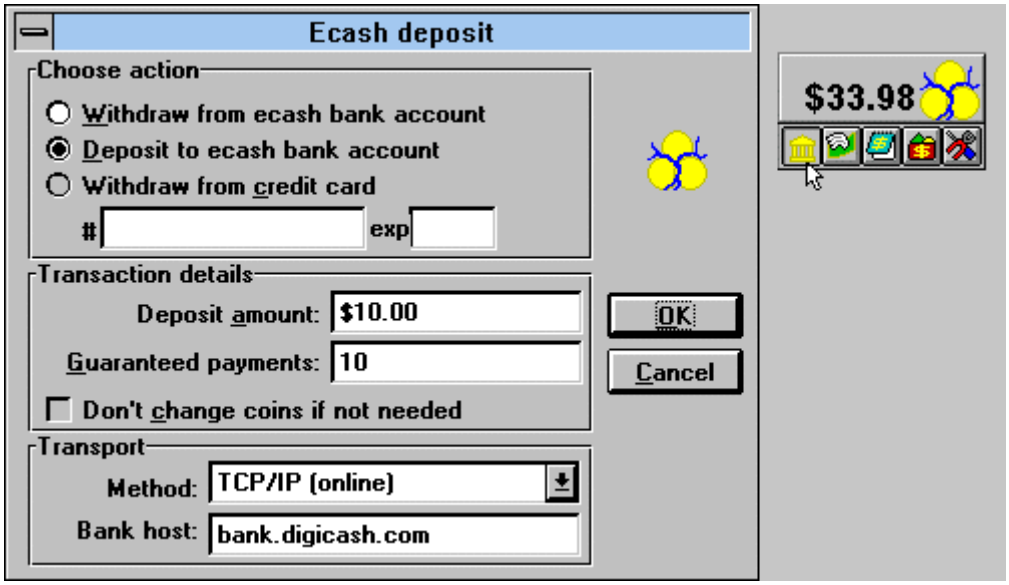
Rysunek V Przyjmowanie nadchodzących pieniędzy (Źródło: DigiCash, ecash client ver 2.1 dla Windows).

Można także określić odpowiednie ustawienia domyślne na przyszłość.



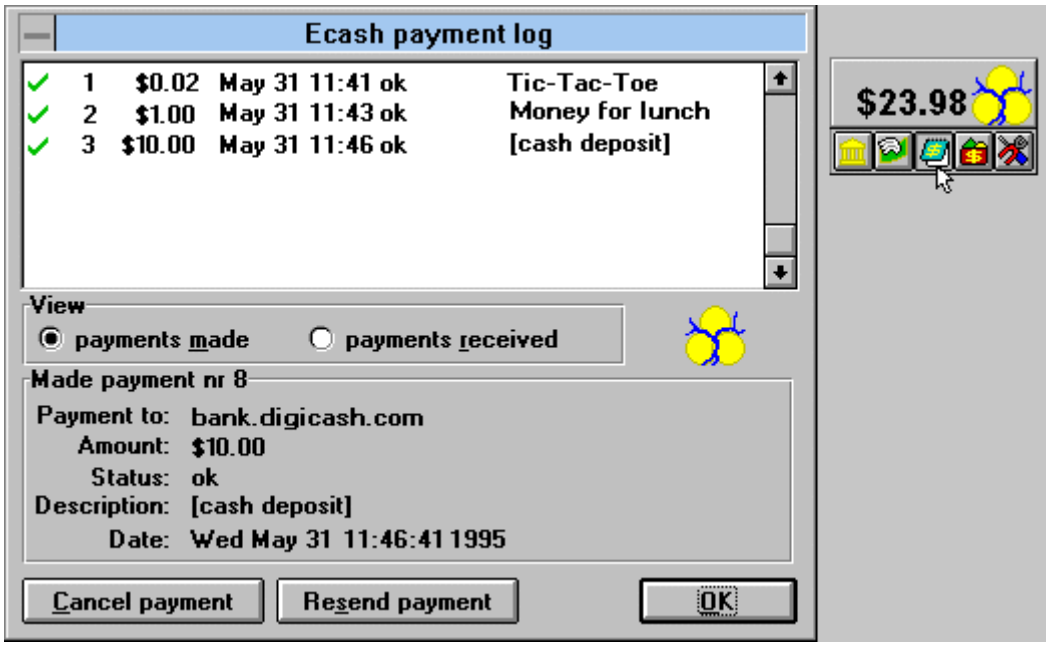
Rysunek W Ustawienia domyślne odnośnie nadchodzących transferów Ecash (Źródło: DigiCash, ecash client ver 2.1 dla Windows).

Pieniądze możemy przechowywać do czasu upłynięcia daty ich ważności. Idąc w drugą stronę, elektroniczne pieniądze można przesłać z powrotem do banku. Faxem, telefonicznie lub poprzez email możemy zażądać, by pieniądze były zamienione w „prawdziwe" dolary, do wykorzystania w konwencjonalny sposób, np. do wypłacenia lub przesłania na inne konto.



Rysunek X Deponowanie Ecash na koncie w banku (Źródło: DigiCash, ecash client ver 2.1 dla Windows).

Naturalnie program umożliwia przeglądanie historii wszystkich płatności, depozytów i transferów.



Rysunek Y Strona debetowa konta bankowego klienta, z zaznaczonymi wszystkimi płatnościami (Źródło: DigiCash, ecash client ver 2.1 dla Windows).

Obecnie Mark Twain Bank przyjmuje 25 różnych walut, które mogą być zdeponowane na koncie służącym do operacji na elektronicznych pieniądzach. Jak na razie Ecash jest denominowany w dolarach amerykańskich, ale Mark Twain Bank planuje z czasem emitować go także innych w walutach i pochodnych, takich jak ECU, SDR lub w pieniądzach opartych na metalach szlachetnych.

Aczkolwiek elektroniczne pieniądze można uznać za potencjalnie pełnoprawną formę płatności internetowych, Ecash z Mark Twain Bank dalej jest w fazie testów. Oferta ograniczona jest do 10 000 użytkowników. Firma przyznaje, że nie ma stuprocentowej gwarancji bezpieczeństwa i ostrzega, że możliwy jest atak na system bądź prywatne oprogramowanie klienta. Posiadane pieniądze należy traktować tak jak gotówkę, która może zostać skradziona. Dlatego bank doradza przechowywanie w domu tylko niewielkich sum. System nie działa jeszcze 24 godziny na dobę. O planowanych operacjach klient musi informować z wyprzedzeniem.

Elektroniczne pieniądze to ciąg cyfr. Ecash składa się z elektronicznych monet, z których każda ma swoją wartość i numer seryjny. Oprogramowanie elektronicznego portfela automatycznie pobiera z banku monety o określonych nominałach, tak by ich suma tworzyła transfer o żądanej wartości. Podobnie przy płaceniu oprogramowanie automatycznie wybiera odpowiednie monety składające się na wartość transakcji.

Gdy sprzedający otrzymuje pieniądze od kupującego, są one wysyłane automatycznie do emitującego je banku. Bank trzyma w bazie danych numery wszystkich emitowanych przez siebie i już wydanych przez klientów elektronicznych monet. Jeżeli ktoś próbuje wydać 2 razy monetę o tym samym numerze, bank to wykryje i anuluje transakcję. Podobnie przy transferach pomiędzy dwiema osobami, program odbiorcy pieniędzy automatycznie przesyła je do swojego banku, który sprawdza, czy są one prawdziwe. Jeżeli wysyłający korzysta z pieniędzy innego banku niż przyjmujący, bank odbiorcy w celu weryfikacji skontaktuje się elektronicznie z bankiem wysyłającego. Przychodzące pieniądze są automatycznie nagrywane na twardy dysk przyjmującego, chociaż mogą być także automatycznie deponowane bezpośrednio na jego koncie.

W takim schemacie wydawałoby się, że bank trzymający w swojej bazie danych numery pieniędzy będzie w stanie kontrolować, kto na co je wydaje. Aby temu zapobiec i umożliwić kupującemu pełną anonimowość, w elektronicznych pieniądzach wykorzystany został algorytm „ślepego podpisu” (blind signature). Polega on na tym, że pieniądze generowane są w sposób losowy przez oprogramowanie klienta i wysyłane do banku, który przystawia do nich elektroniczny stempel, określający ich wartość i potwierdzający ich prawdziwość. Bank nie ma jednak możliwości poznania cech charakterystycznych konkretnych monet. Podczas późniejszej weryfikacji może on jedynie przeczytać swój własny stempel walidujący. Dzięki temu bank nie jest w stanie przyporządkować sprawdzanej przez siebie monety konkretnej osobie.

2.3.2. NetCash

Inną technologią elektronicznych pieniędzy jest NetCash, rozwijany przez Information Sciences Institute z Uniwersytetu Południowej Kalifornii. NetCash jest w fazie testów, nie jest eksploatowany komercyjnie. Tak jak w przypadku DigiCash, klient posiada oprogramowanie tutaj nazywane wirtualnym portfelem (virtual wallet), umożliwiające przechowywanie pieniędzy, tutaj nazywanych kuponami (NetCash coupons), na komputerze osobistym. Kupony nominowane są w USD. Płatność następuje poprzez wysyłanie pieniędzy pocztą elektroniczną.

Kupon NetCash to ciąg znaków określających jego wartość i numer, np.: *NetCash US$ 10.00 A123456B789012C.* Każdy, kto zna numer kuponu, może się nim posłużyć do dokonania płatności. Numerów własnych kuponów należy więc pilnie strzec.

W systemie NetCash stworzony został NetBank, za pośrednictwem którego użytkownik może zamieniać prawdziwe dolary na NetCash i odwrotnie. Opłata za każdą zamianę to dwa procent jej wartości. Nie ma opłat transakcyjnych za poszczególne zakupy. W NetCash można się zaopatrywać kupując je w NetBank poprzez zwykłą pocztę (czek lub money order) lub poprzez WWW/pocztę elektroniczną. Należy tylko wypełnić odpowiedni formularz w WWW, po jego wysłaniu NetBank natychmiast automatycznie przyśle nam pocztą elektroniczną kupon NetCash odpowiedniej wartości. Ma on status „pending" oznaczający, że do czasu rozliczenia czeku przez NetBank (do 10 dni) dany kupon nie jest w pełni gwarantowany jako mający pokrycie.

Kupon NetCash można rozmienić na drobne poprzez email, wysyłając numer kuponu z poleceniem jego zamiany na odpowiednio mniejsze nominały. Służy do tego polecenie „change", np. *NetCash US$ 1.00 A123456B789012C /Change 4 Quarters* zamienia 1 USD na 4 kupony, każdy o wartości 25 centów. Płatności dokonujemy poprzez email, przesyłając sprzedawcy numer NetCash kuponu lub poprzez WWW. Weryfikację, czy

otrzymaliśmy ważne pieniądze, przeprowadza NetBank. Odbiorca wysyła do NetBank otrzymany kupon, razem z poleceniem Accept, np.: *NetCash US$ 12.50 A321456B543876C /Accept.*

NetBank dokonuje weryfikacji, czy kupon istnieje naprawdę i czy nie był już użyty. Jeżeli kupon jest aktualny, NetBank przesyła potwierdzenie razem z nowym numerem kuponu, znanym tylko jego bieżącemu posiadaczowi. Stary kupon wycofywany jest z obiegu. Komenda „accept" służy także do łączenia kilku kuponów w jeden, o sumie ich wartości. Komendą „verify" można sprawdzić, czy dany kupon jest prawdziwy, bez zamiany jego numeru. Komenda „deposit" np. *NetCash US$ 2.20 C432156D765432E /Deposit 123456* przelewa pieniądze z kuponu o podanym numerze na podany numer konta (123456).

System ten ma kilka słabości, do pewnego stopnia charakterystycznych także dla innych rozwiązań elektronicznych płatności. Z faktu, że system jest scentralizowany, wynika, że funkcjonowanie systemu możliwe jest tylko wtedy, gdy w sieci dostępny jest serwer NetBanku. Jego wyłączenie uniemożliwi weryfikację pieniędzy. Przesyłanie pieniędzy NetCash odkrytą pocztą jest bardzo niebezpieczne. Wiadomość może być przechwycona po drodze i pieniądze skradzione. Wszelka korespondencja z NetBank może być kodowana np. przy użyciu popularnego systemu szyfrowania poczty elektronicznej PGP. Wydaje się, że o ile projekt NetCash ma być kontynuowany, kwestie te będą musiały zostać rozwiązane.

2.4. KARTY PŁATNICZE

Niektórzy wierzą, że czysto programistyczne metody płatności przez Internet nigdy nie będą wystarczająco bezpieczne. Metodą po części konkurencyjną, po części uzupełniającą inne rozwiązania jest wykorzystanie „Smart Cards", czyli kart inteligentnych, zwanych też chipowymi. W tej metodzie pieniądze przechowywane są w układach scalonych na karcie. Płatność poprzez Internet następuje przez wsunięcie karty do podłączonego do komputera osobistego czytnika. Za każdym razem, gdy karta jest użyta do transakcji poprzez Internet, układ scalony karty generuje unikalny podpis elektroniczny, rozpoznawany przez inną kartę uczestniczącą w transakcji, gwarantujący legalność operacji. Inteligentne karty mają wyeliminować lub poważnie ograniczyć

transakcje gotówkowe, które obecnie dominują w transakcjach detalicznych, nawet w wysoko rozwiniętych krajach zachodnich.

Zastosowanie kart płatniczych ma dużo szerszy wymiar niż płatności internetowe. Mają być stosowane co regulowania codziennych transakcji gotówkowych i kredytowych (takich jak karty kredytowe, debetowe, typu „charge" i inne), jako karty telefoniczne, parkingowe, bilety komunikacji miejskiej etc. Zalety karty w postaci małych wymiarów, niskiej ceny i potencjalnie dużej bazy klientów predestynują ją do pełnienia istotnej roli w zinformatyzowanym społeczeństwie końca XX wieku.

Poprzez elektroniczny portfel lub czytnik kart pieniądze mogą być przesyłane pomiędzy osobami prywatnymi, zupełnie tak jak gotówka. Elektroniczny portfel (electronic wallet) jest intensywnie rozwijanym urządzeniem, mającym zintegrować funkcje płatnicze kart, komunikacyjne telefonów komórkowych i inne. Jest on rozwijany m.in. w ramach *Project CAFE*[20], będącego częścią programu Unii Europejskiej *ESPRIT*. Taki elektroniczny portfel mógłby być używany do wszelkiego typu opłat, jako końcówka serwisów informacyjnych, identyfikator osobisty, klucze, karta medyczna etc. Ma to być elektroniczne urządzenie kieszonkowe, zbliżone wielkością do przenośnych kalkulatorów. Właściwym nośnikiem pieniędzy będą inteligentne karty płatnicze, jednorazowe lub wielokrotnego zapisu. Komunikacja z urządzeniami zewnętrznymi (kasami, innymi portfelami) następować ma w podczerwieni, podobnie jak w pilotach w sprzęcie RTV.

Rysunek Z Jeden z prototypowych modeli elektronicznego portfela. Oprócz klawiszy numerycznych i pomocniczych ma klawisze: zabezpieczania dostępu, wyboru waluty, przeglądu ostatnich transakcji, salda, transferu (Źródło: Mondex Corp).

Zastosowanie kart chipowych do transakcji internetowych nie stanie się popularne do czasu rozpowszechnienia tanich i niezawodnych czytników kart magnetycznych przyłączanych do komputerów osobistych. Alternatywą są złącza PCMCIA i standardowe połączenia na podczerwień pomiędzy urządzeniami komputerowymi.

[20] http://www.cwi.nl/cwi/projects/cafe.html

Firmą bardzo aktywnie promującą zastosowanie inteligentnych kart w transakcjach internetowych jest Mondex[21] udzielający licencji na swoje rozwiązania bankom i instytucjom finansowym na całym świecie.

2.4.1. Mondex

Mondex jest producentem karty Mondex Card. Jest to plastikowa, inteligentna karta płatnicza (smart card), na której przechowywane są pieniądze, maksymalnie w pięciu różnych walutach. Pieniądze przechowywane są w postaci elektronicznej w specjalnie zaprogramowanym układzie scalonym, który umożliwia ich uzupełnianie poprzez linie telefoniczne i nową generację bankomatów. Aktualną sumę pieniędzy na karcie można sprawdzić za pomocą bardzo prostego czytnika, nasadzanego na kartę.

Rysunek AA Mondex POS Terminal, płatność dokonuje się poprzez wsunięcie karty do czytnika.

Rysunek BB Czytnik stanu karty, kwota zapisana na karcie pokazywana jest na miniaturowym wyświetlaczu.

Rysunek CC Mondex telefon, pełni funkcję osobistego bankomatu.

(Źródło: Mondex Corp.)

Klienci posługujący się kartą Mondex będą mogli nią płacić tak jak gotówką w akceptujących ją punktach. Będą one miały swoje własne karty, na których będą się

[21] http://www.worldserver.pipex.com/mondex/

akumulować wpłaty klientów. W dowolnym momencie pieniądze będą mogły zostać przelane (przez Mondex telefon) na konto bankowe.

Karta może być zabezpieczona za pomocą kodu dostępu, tak by używać jej mógł tylko jej właściciel. Jako że karta rejestruje w wewnętrznej pamięci wszystkie dokonane transakcje i cechy kart sprzedawców, właściciel może sprawdzić, gdzie i po co użył karty.

Karta Mondex ma zalety gotówki poszerzając je o wiele innych pożądanych cech:

- możliwe są transfery osobiste, dokonuje się tego za pomocą Mondex portfela, a na większe odległości za pomocą Mondex telefonu;
- nie wymagana jest instytucja pośrednicząca ani autoryzacja on-line w punktach sprzedaży;
- regulacja należności następuje natychmiast;
- mała karta jest wygodniejsza w zastosowaniu niż gotówka;
- nie trzeba nosić ze sobą drobnych;
- łatwy jest dostęp do konta w banku: poprzez Mondex telefon łatwo uzupełniać pieniądze na karcie;
- płacić można za dowolnej wielkości zakupy (karty kredytowe czy czeki z reguły służą do zakupów o większej wartości);
- automatycznie prowadzona jest rejestracja wszystkich wydatków;
- kartę można zabezpieczyć przed nieautoryzowanym użyciem;
- karta jest wielowalutowa.

Zaletami dla sprzedawców jest szybsza obsługa klienta, gdyż nie wymagany jest podpis czy autoryzacja on-line, łatwe przelewanie pieniędzy z i na konto z własnej karty, ominięcie kosztów związanych z przechowywaniem, liczeniem i transportowaniem gotówki i czeków, automatyczna rejestracja danych o transakcjach. Jako proste terminale POS (point of sale) mogą być używane podręczne elektroniczne portfele.

Ponieważ karta zastępuje gotówkę, podobnie zachowuje się w przypadku jej zgubienia- pieniądze przepadają. Niemniej każda karta ma 16-cyfrowy numer, zarejestrowany

przez bank wystawcy, tak więc w przypadku jej znalezienia właściciel może ją odzyskać. Znalazca może uzyskać nagrodę w banku wystawcy. Karta uszkodzona podlega wymianie przez bank.

Zastosowanie karty do transakcji poprzez Internet jest bardzo proste. Poprzez przeglądarkę WWW łączymy się z interesującą nas firmą. Po wybraniu z katalogu interesujących nas produktów czy usług będziemy proszeni o włożenie karty Mondex do czytnika kart, podłączonego do komputera przez port szeregowy. System upewni się czy urządzenie sprzedawcy istnieje i przeleje odpowiednią sumę pieniędzy (w wybranej przez nas walucie) na kartę sprzedawcy. Jest to wygodne dla klienta, który nie musi za każdym razem ręcznie wpisywać danych swojej karty kredytowej.

Karta Mondex jest obecnie w fazie zaawansowanych testów. W Wielkiej Brytanii technologia ta wprowadzana jest przez połączone konsorcjum banków NatWest i Midland, korzystające z pomocy różnych podwykonawców, takich jak British Telecom, który dostarcza Mondex telefony. Projekt pilotowy wdrażany jest w mieście Swindon, wybranym ze względu na swoją reprezentacyjność brytyjskiego społeczeństwa. W ciągu 2 lat trwania projektu ma on objąć blisko 40 000 konsumentów i 1000 sprzedawców. Inne testy mają się też rozpocząć w Kanadzie i na Dalekim Wschodzie.

Upowszechnieniu karty sprzyja fakt, że przy zachowaniu odpowiednich standardów ISO karty różnych producentów będą wzajemnie kompatybilne.

Idea bezpiecznych transakcji internetowych przy użyciu kart chipowych jest rozwijana także przez innych producentów i instytucje finansowe. Szczególnie ważne wydaje się być porozumienie[22] Europay International[23] z IBM Corporation[24].

22 http://www.europay.com/1995/ph5rtt45.htm
[23] http://www.europay.com/
[24] http://www.ibm.com/

2.4.2. Europay

Europay dostarcza bankom pełny zakres produktów i usług płatniczych, takich jak czeki podróżne, bankomaty, elektroniczne terminale POS, karty kredytowe i debetowe. Wraz z MasterCard jest właścicielem European Payment Systems Services S.A., firmy dokonującej autoryzacji, rozliczeń i clearingu kart płatniczych.

Porozumienie z IBM przewiduje połączenie elektronicznego portfela, produktu Europay z rozwijanym przez IBM bezpiecznym protokołem płatniczym iKP[25]. Płatności będzie się dokonywać poprzez włożenie karty płatniczej z zapisanymi na niej pieniędzmi do czytnika karty, podłączanego do komputera, telefonu czy telewizora. Obecnie prowadzony jest program pilotowy. Inicjatywa ma umożliwić bezpieczne transakcje poprzez WWW, szczególnie najpopularniejsze w Internecie mikro-płatności. Transakcje o większej wartości będą także możliwe- karty kredytowe i debetowe zaczynając od 1997 roku poddane mają być konwersji ze standardu karty magnetycznej na kartę chipową.

Karty Europay oprócz płatności internetowych mają być wykorzystywane w płatnej telewizji pay-per-view, komunikacji publicznej, automatach ulicznych, parkingach etc. Zastosowanie inteligentnej karty chipowej ma znacznie zredukować oszustwa i koszt przetwarzania transakcji, m.in. dzięki uniknięciu potrzeby kosztownych połączeń on-line pomiędzy wystawcą a przyjmującym kartę. Układ scalony będzie gwarantował jej autentyczność, a osobisty kod właściciela PIN będzie zapobiegał jej nie autoryzowanemu użyciu.

[25] http://www.zurich.ibm.com/Technology/Security/extern/ecommerce/iKP.html

2.5. INNE

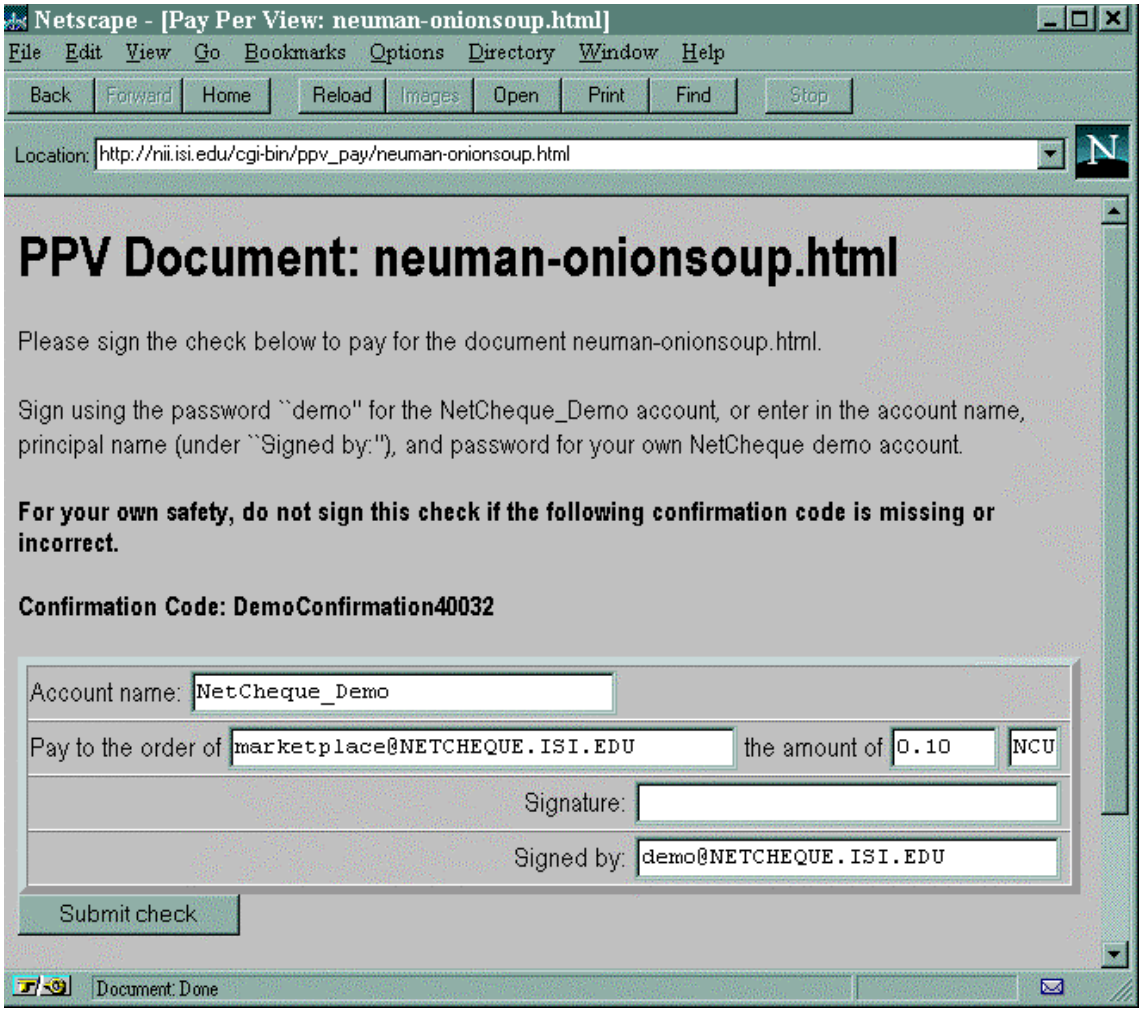
2.5.1. NetCheque

NetCheque[26] jest sposobem elektronicznych płatności internetowych opracowanym przez Instytut Nauk Informacyjnych Uniwersytetu Południowej Kalifornii. Jest on internetowym odpowiednikiem płatności czekami. Używając poczty elektronicznej lub innych protokołów sieciowych użytkownicy mogą dokonywać przelewów z jednego konta na drugie. Do posługiwania się systemem wymagane jest konto na serwerze księgowym NetCheque.

System płatności za pośrednictwem czeków nie jest specjalnie nowatorski. Powszechnie stosowane programy do prowadzenia prywatnych finansów, takie jak Quicken czy Microsoft Money, mają moduły umożliwiające usługi home banking. Poprzez modem programy te łączą się z bankiem, w którym mamy konto i pobierają informacje czy wydają bankowi polecenia. NetCheque jest jednak lepiej zintegrowany z Internetem. Płatność następuje automatycznie wtedy, gdy chcemy skorzystać z jakiejś płatnej usługi internetowej, np. czytać teksty, za przeglądanie których trzeba płacić (pay-per-view).

[26] http://nii-server.isi.edu/info/NetCheque/

Wybieramy interesującą nas usługę za pomocą przeglądarki WWW, po naciśnięciu przycisku „zapłać” uruchomi się aplikacja NetCheque (pay-per-view client). W wersji próbnej można także płacić posługując się tylko i wyłącznie przeglądarką WWW.



Rysunek DD Przykładowa płatność przy użyciu przeglądarki WWW w systemie NetCheque.

Strona WWW, za którą zapłaciliśmy, wyświetlana jest tylko raz. Przy ponownej próbie wyświetlenia system powie, że dany czek został już zużyty. W ten sposób płacić można tylko w wersji testowej, gdyż nie gwarantuje ona żadnego bezpieczeństwa przesyłanych siecią haseł.

System NetCheque dla autentyfikacji posługuje się systemem Kerberos. Do szyfrowania transakcji stosowany jest algorytm symetryczny. Nadaje to systemowi dużą wydajność,

czyniąc go dobrze przystosowanym do mikro-płatności. System jest skalowalny, clearing zapewnia wiele połączonych serwerów.

System NetCheque jest podobny w swoim działaniu do innych systemów. Od długiego czasu jest w fazie testów, nie wiadomo, czy kiedykolwiek będzie używany komercyjnie.

2.5.2. NetBill

NetBill[27] jest kolejnym systemem płatności zaprojektowanym specjalnie z myślą o internetowych mikro-płatnościach. Jest to wspólny projekt Carnegie Mellon University, VISA i Mellon Bank.

Podobnie jak inne schematy internetowych płatności zakłada on istnienie internetowego pośrednika pomiędzy kupującym a sprzedającym, odpowiedzialnego za logistykę i sprawy techniczne. System zapewnia pełne bezpieczeństwo transakcji dzięki prywatności zakupów, bezpiecznej komunikację i możliwości sprawdzenia tożsamości nadawcy.

Korzystający z systemu muszą mieć konto na serwerze NetBill. Konta są powiązane z rachunkami w klasycznych instytucjach finansowych. W przypadku transakcji towary przepływają pomiędzy sprzedającym a kupującym, konto kupującego obciążane jest na sumę zakupu, która powiększa konto sprzedawcy. W razie potrzeby konto kupującego może być powiększone o środki z tradycyjnych rachunków bankowych.

NetBill jest przystosowany do mikro-transakcji, opłaty transakcyjne są bardzo małe (ok. 1 centa z 10-centowej transakcji). System jest w fazie testów i rozwoju, nie wiadomo czy i kiedy będzie stosowany komercyjnie.

[27] http://www.ini.cmu.edu/netbill/

3. BEZPIECZE□STWO W INTERNECIE

3.1. WPROWADZENIE

Elektroniczne płatności są w użyciu od kilkudziesięciu lat. Dotychczas jednak odbywały się poprzez izolowane, bezpieczne sieci finansowe. Internet łącząc komputery klientów z serwerami sprzedawców ma architekturę otwartą. Każdy może się do niego podłączyć. Informacje przysyłane z jednego miejsca do drugiego przechodzą przez wiele komputerów, po drodze do których ktoś może się włamać i zainstalować program, który będzie przechwytywał przesyłane dane.

Bezpieczeństwo danych stanowi największą przeszkodę w szerszej popularyzacji elektronicznego handlu poprzez Internet. Nie zabezpieczone dane przesyłane Internetem mogą zostać przechwycone, odczytane i zmienione. Nie ma mechanizmów weryfikujących tożsamość nadawcy.

Ograniczenia te obchodzi się metodami programistycznymi i sprzętowymi. Ogólnie rzecz biorąc internetowe systemy płatności powinny charakteryzować się następującymi cechami:

- tajność (confidentiality): użytkownik przesyłający dane ma pewność, że będą one dostępne tylko dla upoważnionego odbiorcy; tajność realizuje się przez szyfrowanie danych;
- integralność (integrity): wiadomość nie zostanie przez nikogo zmieniona po drodze; integralność realizuje się przez podpis elektroniczny;
- autentyfikacja (authentication): użytkownik lub organizacja są w stanie udowodnić swoją tożsamość; realizuje się to przez podpis elektroniczny i elektroniczne certyfikaty;
- autoryzacja (authorization): po nawiązaniu kontaktu dostawca jest w stanie określić czy klient ma uprawnienia do zażądanej przez siebie usługi czy zasobów;
- prywatność (privacy): szczegóły transakcji są tajne dla osób postronnych;
- dodatkowe wymagania to powszechność (potencjalnie wszyscy powinni być w stanie używać systemu) i pewność (przerwy w pracy lub przekłamania systemu są niedopuszczalne).

3.2. SZYFROWANIE DANYCH

Najlepszym sposobem zapewnienia bezpieczeństwa danym przesyłanym Internetem jest poddanie ich szyfrowaniu, czyli modyfikacji w oparciu o tajny parametr- klucz szyfrowania. Najogólniej rzecz biorąc stosowane są 2 metody szyfrowania danych: symetryczne (konwencjonalne) i niesymetryczne (metoda klucza publicznego).

3.2.1. Szyfrowanie symetryczne

W metodzie symetrycznej do szyfrowania i odszyfrowania używamy tego samego klucza, co oznacza, że musi on być znany nadawcy i adresatowi przed wysłaniem zaszyfrowanej wiadomości. Najpopularniejsze algorytmy szyfrowania symetrycznego to np. DES (Data Encryption Standard), potrójny DES, IDEA (International Data Encryption Algorithm).

Szyfrowanie symetryczne ma poważne wady. Obie strony muszą znać klucz kodujący, który powinien być przekazany w jakiś bezpieczny sposób poza siecią. Trudno jest to zrobić, gdy komunikujemy się z dużą liczbą osób, o których nic nie wiemy i Internet jest jedyną drogą kontaktu. Ponadto dla każdego użytkownika czy dostarczyciela usług, z którym się kontaktujemy, musimy mieć odmienny klucz. Tak samo dostarczyciel usługi musi pamiętać klucz każdego ze swoich potencjalnych klientów.

Ograniczenia szyfrowania symetrycznego omijane są na dwa sposoby. Jednym z nich jest zastosowanie przez obie kontaktujące się strony pośrednika, do którego oboje mają zaufanie. Pośrednik ten generuje klucze szyfrowania dystrybuowane do obydwu stron.

Inną metodą jest szyfrowanie asymetryczne, znane także pod nazwą metody klucza publicznego.

3.2.2. Szyfrowanie metodą klucza publicznego

Szyfrowanie metodą klucza publicznego (asymetryczne) zapewnia poufność transmitowanych danych i ich integralność (podpis elektroniczny). System ten został

stworzony w 1976 roku przez Whitfielda Diffie i Martina Hellmana. Najczęściej wykorzystywanym algorytmem szyfrowania asymetrycznego jest RSA.

W tym schemacie każdy użytkownik ma dwa klucze: jeden publiczny, który udostępnia innym i drugi prywatny, znany tylko jemu. Znając klucz publiczny nie można odkryć klucza prywatnego. Użytkownik szyfruje wiadomość swoim kluczem prywatnym i kluczem publicznym adresata. Adresat i tylko adresat może odczytać wiadomość swoim kluczem prywatnym i kluczem publicznym nadawcy. Ma on pewność, że tylko oni dwaj znają wiadomość i że sama wiadomość pochodzi od danego nadawcy (wiadomość da się odczytać tylko przy użyciu unikalnego klucza publicznego nadawcy).

Podstawową zaletą szyfrowania metodą klucza publicznego jest zwiększone bezpieczeństwo i wygoda. W szyfrowaniu symetrycznym musimy w jakiś sposób (ręcznie, poza siecią, lub w jakiś inny bezpieczny sposób) przekazać klucz szyfrujący. Przesyłając go siecią ryzykujemy przechwycenie go przez osobę niepowołaną. W szyfrowaniu asymetrycznym klucz prywatny nigdy nie musi być transmitowany przez sieć. Nie jest on nikomu przekazywany. Nie musimy także posiadać oddzielnego klucza do każdego użytkownika, z którym się kontaktujemy. Wystarczy zawsze ten sam nasz klucz prywatny i klucz publiczny danego użytkownika.

W systemie szyfrowania symetrycznego często występuje strona trzecia, przechowująca tajne klucze szyfrujące użytkowników. Tak jest na przykład w systemie Kerberos. Udany atak sieciowych włamywaczy na taką bazę danych oznacza złamanie całego systemu. W systemie klucza publicznego tylko właściciele znają swoje klucze prywatne, co jest znacznie bezpieczniejszym rozwiązaniem. Właściwość ta ma zastosowanie przy jednej z fundamentalnych technik kryptograficznych: elektronicznym podpisie. Podpisując coś swoim kluczem prywatnym użytkownik nie może potem twierdzić, że tego nie zrobił, tłumacząc się, że strona trzecia ujawniła przechowywany przez siebie tajny klucz.

Podstawową wadą szyfrowania asymetrycznego jest jego niska wydajność. Szyfrowanie to jest znacząco powolniejsze niż szyfrowanie symetryczne. Nie nadaje się do

najbardziej intensywnych zastosowań, gdzie naraz musi być przetwarzana duża liczba wiadomości wielu klientów.

3.2.3. Szyfrowanie hybrydowe

Ze względów wydajnościowych w szyfrowaniu najczęściej używa się rozwiązania hybrydowego, łączącego metodę symetryczną z metodą klucza publicznego. Szyfrowania asymetrycznego używa się do przekazania sumy kontrolnej i klucza symetrycznego, który służy do zaszyfrowania całej wiadomości. Technika ta jest stosowana zarówno do systemów zabezpieczających pocztę elektroniczną, takich jak PEM (Privacy Enhanced Mail) czy PGP (Pretty Good Privacy) oraz w protokołach używanych w World Wide Web: SSL i S-HTTP. Takie rozwiązanie nazywa się cyfrową kopertą (digital envelope).

Zarówno szyfrowanie symetryczne jak i niesymetryczne są intensywnie rozwijane. Obie metody wzajemnie się uzupełniają, gwarantując podwyższone bezpieczeństwo. Stosowanie wyłącznie szyfrowania symetrycznego możliwe jest w instytucjach zamkniętych, typu bank, gdzie istnieje dobrze chronione centralne repozytorium kluczy szyfrujących, lub w sytuacji, gdy kontaktujące się strony komunikują się regularnie innymi metodami niż sieć, co umożliwia wymianę klucza szyfrującego. Metoda klucza publicznego nadaje się lepiej do środowiska otwartego, gdzie użytkownicy nie znają się wzajemnie i kontaktują tylko poprzez sieć.

3.3. PODPIS ELEKTRONICZNY

Dla bezpieczeństwa komunikacji i handlu w Internecie fundamentalną sprawą jest pewność, że otrzymana wiadomość nie została w żaden sposób po drodze zmieniona. Osiąga się to poprzez podpis elektroniczny, możliwy dzięki zastosowaniu szyfrowania metodą klucza publicznego. Podpis elektroniczny, ewentualnie uzupełniony o certyfikat tożsamości gwarantuje, że dana wiadomość została wysłana przez określoną osobę i nie została w żaden sposób zmieniona po drodze.

W technice tej specjalny algorytm matematyczny redukuje całą wiadomość do krótkiej kontrolnej wartości numerycznej. Jakakolwiek zmiana w oryginalnym dokumencie powoduje nieprzewidywalną zmianę wartości kontrolnej. Taką wartość kontrolną

szyfrujemy przy użyciu naszego klucza prywatnego i dołączamy do przesyłanej wiadomości. Odbiorca samodzielnie generuje wartość kontrolną z otrzymanej wiadomości i porównuje ją z odszyfrowaną wartością kontrolną, którą otrzymał w podpisie. Jeżeli obie wartości się zgadzają, to odbiorca ma pewność, że wiadomość pochodzi od posiadacza danego klucza publicznego i nie została w żaden sposób zmieniona po drodze.

Najpopularniejsze algorytmy elektronicznego podpisu to: MD5 produkcji RSA i SHA produkcji NIST (National Institute of Standards and Technology).

3.4. AUTENTYFIKACJA

Autentyfikacja oznacza możliwość stwierdzenia, czy dany użytkownik naprawdę jest tym, za kogo się podaje. Najlepiej realizuje się ją poprzez szyfrowanie asymetryczne.

3.4.1. Urzędy certyfikujące

Dla potrzeb autentyfikacji niezbędne jest istnienie bezpiecznej strony trzeciej, nazywanej urzędem certyfikującym (certification authority). Urzędy certyfikujące mają podstawowe znaczenie dla dystrybucji i weryfikacji kluczy publicznych użytkowników. Za pośrednictwem urzędu użytkownicy muszą być w stanie łatwo sprawdzać wiarygodność kluczy innych użytkowników i rozpowszechniać swoje własne klucze publiczne. Nadając zaszyfrowaną wiadomość musimy być pewni, że dysponujemy właściwym kluczem publicznym adresata. Jeśli komuś uda się podmienić klucz publiczny naszego rozmówcy to będzie w stanie odczytywać adresowane do niego wiadomości. Będzie się także mógł pod niego podszywać, wysyłając w jego imieniu pocztę elektroniczną. Klucze publiczne muszą być dystrybuowane w taki sposób by osoby czy firmy nigdy nie kontaktujące się z posiadaczem danego klucza mogły mieć pewność, że należy on właśnie do danej osoby. Służą do tego cyfrowe certyfikaty, wydawane są one przez urzędy certyfikujące. Najprostszy certyfikat zawiera klucz publiczny i nazwę użytkownika. Często ma także datę ważności, nazwę urzędu certyfikującego i numer seryjny. Może zawierać także inne informacje. To wszystko jest podpisane kluczem prywatnym urzędu. Proponowanym standardem certyfikatów jest międzynarodowy standard ITU-T X.509. Mogą być one zapisywane i czytane przez dowolną aplikację zgodną z normą X.509.

Naturalnie użytkownicy muszą mieć do danego urzędu zaufanie. Dodatkowo rozwiązanie musi być skalowalne. Wraz ze wzrostem zasobów i użytkowników nie mogą pogarszać się parametry pracy systemu. Rozwinięta powinna być hierarchiczna struktura urzędów certyfikujących, w których urzędy niższego szczebla są certyfikowane przez te stojące ponad nimi, które z kolei są autoryzowane przez te jeszcze wyżej i tak dalej, aż do samego szczytu, gdzie jest urząd autoryzujący najwyższego poziomu, któremu się ufa z założenia. Urzędy certyfikujące mogą być podzielone np. geograficznie. Utworzenie hierarchicznych, ufających sobie i wymieniających informacje urzędów, z których jedne autoryzują drugie, wymaga czasu i globalnych ustaleń odnośnie metod współpracy. Na razie realizowane jest to w skali mikro, jeden zaufany użytkownik PGP potwierdza autentyczność klucza publicznego drugiemu i nie ma jednej centralnej instytucji wydającej certyfikaty.

Bezpieczeństwo urzędu certyfikującego jest czynnikiem krytycznym bezpieczeństwa jego użytkowników. Wobec niemożności prostego złamania zakodowanych wiadomości większość ataków hackerów będzie wymierzona prawdopodobnie w same urzędy. Urząd autentyfikacyjny może, ale nie musi być włączony do sieci. Jeśli nie jest, zwiększa to jego bezpieczeństwo, jako że prościej jest chronić system nie narażony bezpośrednio na włamanie z sieci. Oznacza to jednak mniejszą elastyczność w udzielaniu nowych certyfikatów, dlatego często takie odpowiednio zabezpieczone urzędy dostępne są on-line.

Oprócz odpowiedniej długości klucza, dodatkowym czynnikiem sprzyjającym jego bezpieczeństwu jest czasowość jego obowiązywania. Zmniejsza to ryzyko złamania klucza i ewentualnych strat, jeżeli coś takiego nastąpi. Oprogramowanie deszyfrujące powinno sprawdzać automatycznie okres ważności klucza i nie akceptować przeterminowanych. Po wygaśnięciu ważności starego klucza użytkownik powinien postarać się o nowy, zwykle większej długości niż poprzedni, co kompensuje wzrost mocy obliczeniowej komputerów, które mogą być użyte do złamania klucza. Aktualnie RSA sugeruje klucze długości 768 bitów dla zastosowań osobistych, 1024 bity dla celów biznesowych i 2048 dla zastosowań specjalnych, np. dla urzędów certyfikujących.

Wielkości te będą ulegały zwiększeniu wraz ze wzrostem mocy obliczeniowej komputerów.

Cykl życia kluczy szyfrujących wygląda następująco:

- generacja i ewentualna rejestracja klucza publicznego w urzędzie certyfikującym;
- dystrybucja klucza publicznego;
- ewentualne odwołanie ważności klucza (np. gdy podejrzewamy, że ktoś poznał nasz klucz prywatny);
- wygaśnięcie ważności klucza.

Dana osoba może mieć kilka par kluczy, np. oddzielne do działalności zawodowej i prywatnej, swoje klucze mogą też mieć instytucje. Klucze generowane mogą być indywidualnie przez samych użytkowników, a następnie przedstawiane do rejestracji, lub generowane dla użytkowników przez zajmującą się tym w danej organizacji osobę, która troszczy się dalej o rejestracje i wszystkie kwestie porządkowe. Najlepiej gdy urzędem certyfikującym jest organizacja w jakiś sposób związana z użytkownikami, np.: przedsiębiorstwo dla swoich pracowników czy uniwersytet dla swoich studentów. Urzędy muszą dawać gwarancje prawdziwości sygnowanych przez siebie danych, tak więc powinny wymagać przy rejestracji użytkownika jego dowodu tożsamości.

Ponieważ stracenie klucza prywatnego oznacza, że włamywacz może czytać adresowaną do nas korespondencję i podpisywać się za nas, klucz ten należy starannie chronić. Nie powinien on być nigdy przechowywany w postaci odkrytego tekstu. Najprościej jest zaszyfrować go na hasło i przechowywać na dysku. Najlepiej jeśli dysk nie jest widzialny z sieci, np. jest to nasz dysk lokalny. O ile dany komputer używany jest przez wielu użytkowników, klucz przechowywać można na dyskietce lub jeszcze lepiej na zapisywalnej karcie magnetycznej.

Jeżeli użytkownik obawia się, że jego klucz prywatny dostał się w niepowołane ręce, musi zgłosić to natychmiast swojemu urzędowi certyfikującemu, który umieści dany klucz na liście kluczy anulowanych. Listy te są wymieniane pomiędzy urzędami. Weryfikując podpis odbiorca powinien sprawdzić, czy dany podpis nie znajduje się na liście certyfikatów anulowanych.

Powstające urzędy certyfikujące przechowywać będą zarówno klucze publiczne użytkowników, jak i ich certyfikaty. Jednym z dostawców oprogramowania realizującego funkcje urzędu autoryzacyjnego jest VeriSign[28], Inc.

3.4.2. Kerberos

Autentyfikacja może być także zrealizowana bazując na szyfrowaniu symetrycznym, za pomocą systemu Kerberos. Pomiędzy odbiorcą a nadawcą występuje zapewniający weryfikację serwer autoryzacyjny Kerberosa. Zarówno odbiorca, jak i nadawca muszą być uprzednio zarejestrowani w serwerze autoryzacyjnym i mieć swoje hasła użytkownika. Nadawca chcący skontaktować się z odbiorcą wysyła do serwera autoryzacyjnego wiadomość zawierającą nazwę swoją i odbiorcy razem z informacją dodatkową. Serwer autoryzacyjny odpowiada przypadkowo wygenerowanym kluczem sesji zwracanym nadawcy w sposób zaszyfrowany za pomocą zarejestrowanego uprzednio hasła nadawcy. Kluczowi sesyjnemu towarzyszy zaszyfrowany kluczem odbiorcy bilet (ticket) zawierający nazwę nadawcy i klucz sesyjny. Zarówno klucz sesyjny, jak i bilet są ważne tylko przez określony czas. Nadawca chcący się zidentyfikować przed odbiorcą przesyła mu bilet z załączonym stemplem czasowym zaszyfrowanym kluczem sesyjnym z biletu. Odbiorca odszyfrowuje za pomocą własnego klucza bilet, wydobywa zaszyty w nim klucz sesyjny i odczytuje stempel czasu. Gdy stempel czasu jest aktualny, odbiorca wie, że wiadomość została wysłana przez kogoś, kto zna klucz sesyjny. A ponieważ klucz sesyjny wystawiony był tylko określonemu w bilecie nadawcy, identyfikuje to jednoznacznie nadawcę. W przypadku, gdyby autentyfikacji wymagał także nadawca, odbiorca wydobywa stempel czasowy, zaszyfrowuje go kluczem sesyjnym i zwraca do nadawcy. Do dalszej komunikacji pomiędzy nadawcą a odbiorcą służy klucz sesyjny, realizujący szyfrowanie symetryczne.

3.5. AUTORYZACJA

Autoryzacja daje możliwość określenia, czy dana osoba po ustaleniu jej tożsamości (autentyfikacja) ma prawo do żądanej przez siebie usługi czy operacji. Zwykle ma to charakter lokalny dla danej maszyny, tj. istnieje jakaś lista kontrolna przypisująca

określonym użytkownikom i ich grupom pewne prawa do plików, aplikacji, zasobów etc. Jest to rozwiązanie raczej dla sieci lokalnych niż lokalnych użytkowników.

Handel elektroniczny wymusza rozwiązanie rozproszone, gdzie istnieje wiele serwerów autoryzacyjnych, wzajemnie się ze sobą komunikujących. Wystawiałyby one podpisywane certyfikaty określające przynależność do grup czy pozwolenie na dokonanie danych usług. Korzystaliby z nich dostawcy serwisów i usług, sprawdzając podpis instytucji autoryzującej i zgodność zażądanej przez użytkownika usługi z przyporządkowanymi mu prawami. Eliminuje to konieczność trzymania przez każdego dostawcę usług swojej własnej listy lokalnej użytkowników. Rozwiązanie to jest elastyczniejsze i łatwiejsze w zarządzaniu. Obecnie realizowanych jest kilka projektów mających udostępnić rozproszone usługi autoryzacyjne.

3.6. PRYWATNOŚĆ

W sytuacji, gdy sieć jest powszechnie wykorzystywana do wyszukiwania informacji i robienia zakupów, ktokolwiek mający dostęp do historii zakupów klienta może łatwo poznać jego zainteresowania i nawyki. Podobnie firmy mogłyby szpiegować działania konkurencji.

Klient powinien mieć prawo do prywatności swoich transakcji. Technologią to umożliwiającą jest ślepy podpis (blind signature). Zastosowany został w elektronicznych pieniądzach, uniemożliwiając ich przyporządkowanie konkretnej osobie. Podobne właściwości ma mieć płatność kartą opracowaną w ramach *Project CAFE*. Tam, gdzie płatność następuje poprzez kartę kredytową (np. First Virtual), czy występuje pośrednik zamieniający jedną postać pieniędzy na drugą (np. NetCash) użytkownik powinien mieć prawo do decydowania, jak dużo informacji o sobie chce ujawnić (poza tymi niezbędnymi służącymi do zapłaty) i jaki będzie ich dalszy los. Wydaje się, że w trosce o klienta usługodawcy będą oferować rosnącą anonimowość swoim klientom. Nieuczciwych sprzedawców będzie można ścigać z ramienia prawa.

[28] http://www.verisign.com/

3.7. TECHNOLOGIE BEZPIECZNEJ TRANSMISJI DANYCH

Na bazie szyfrowania symetrycznego i asymetrycznego stworzono szereg technologii, które umożliwiają internetowy handel i płatności. Realizują one wymogi bezpieczeństwa w WWW, poczcie elektronicznej i innych usługach Internetu. Własne zintegrowane systemy płatności i dostarczania usług oferują firmy takie jak DigiCash, CyberCash, First Virtual, NetCheque, NetBill, OpenMarket i inne. Występuje też cała gama innych, mniej lub bardziej różniących się proponowanych protokołów elektronicznych transakcji, np. iKP opracowany przez IBM czy Secure Courier produkcji Netscape'a.

3.7.1. SSL

Secure Sockets Layer (SSL) jest protokołem opracowanym przez Netscape Communications[29], czołowego producenta przeglądarek WWW. Jest to protokół mający zapewnić bezpieczną transmisję danych poprzez Internet. Działa na poziomie sesji pomiędzy protokołami usług sieciowych (obecnie HTTP, a wkrótce także Telnet, NNTP, FTP, Gopher) a głównym protokołem komunikacyjnym w Internecie, TCP/IP. Bezpieczeństwo transmisji realizowane jest poprzez szyfrowanie danych, autentyfikację serwera, integralność wiadomości i opcjonalnie, autentyfikację klienta. Dane są bezpieczne tylko w momencie transmisji, tj. nie są szyfrowane, gdy przechowuje się je na serwerze.

Inicjacja sesji SSL następuje poprzez tzw. handshake. Jego wynikiem jest uzgodnienie przez przeglądarkę i serwer poziomu bezpieczeństwa, którego dalej będą używać i dokonanie autentyfikacji. Najpierw serwer przesyła na żądanie klienta swój certyfikat i preferencje odnośnie kodowania. Klient generuje klucz główny, który szyfruje kluczem publicznym serwera i przesyła do serwera. Serwer odczytuje klucz, autentyfikuje się wobec klienta przesyłając wiadomość zakodowaną tym kluczem, po czym generuje klucze pokrewne, które służą do szyfrowania przesyłanych następnie danych. Opcjonalnie może wystąpić faza autentyfikacji klienta, kiedy to na żądanie serwera klient przesyła swój podpis elektroniczny i certyfikat klucza publicznego.

[29] http://www.netscape.home

Standard SSL jest wspierany przez najpopularniejszą w Internecie (60-80% rynku) przeglądarkę WWW Netscape Navigator produkcji Netscape Communications. Ma ona dodatkowy sposób łączenia się z serwerem WWW, poprzez „https" (w odróżnieniu od normalnego „http"), oznaczające protokół SSL, działający ponad HTTP i TCP/IP. Przeglądarka Netscape Navigator ma wbudowane autoryzujące klucze publiczne uznawanych urzędów autoryzujących (Certificate Authority). Pozwala to przeglądarce na upewnienie się, czy serwer, z którym nawiązała kontakt, jest autoryzowany przez któryś z tych urzędów. Standardowym numerem portu jest 443 (standardowo, dla nie zabezpieczonego HTTP jest to 80). Jako że SSL i HTTP są różnymi protokołami komunikującymi się poprzez różne porty serwera, możliwe jest ich równoczesne używanie. Część stron może być niezabezpieczona, zabezpieczone SSL mogą być tylko strony, gdzie klient dokonuje płatności.

SSL korzysta z wielu algorytmów szyfrujących. W fazie nawiązania sesji stosowany jest RSA, a później, przy wymianie danych RC2, RC4, IDEA, DES, potrójny DES, MD5 (elektroniczny podpis). Certyfikaty kluczy publicznych stosują się do normy X.509.

SSL jest najczęściej obecnie stosowanym standardem ochrony danych w WWW. Ma poparcie największych firm branży. Obecnie używana jest wersja 2.0, chociaż Netscape przekazał już do IETF (Internet Engineering Task Force) projekt wersji 3.0. Zastrzeżenie może budzić wymuszony amerykańskimi restrykcjami eksportowymi zaledwie 40 bitowy klucz szyfrujący, stosowany w międzynarodowej wersji przeglądarki. Zabezpieczenie to zostało w sierpniu 1995 roku złamane przez pewnego francuskiego studenta. Użył on do tego 120 stacji roboczych i 2 superkomputerów. Odgadywały one kolejne możliwe hasła i porównywały następnie z zaszyfrowaną wiadomością. Odkrycie właściwego hasła zajęło 8 dni, w ciągu tego czasu komputery wypróbowały 500 miliardów kombinacji klucza. Zarówno ta, jak i inne udane próby złamania 40 bitowego zabezpieczenia zostały szeroko nagłośnione i obniżyły zaufanie pokładane w SSL. Netscape tłumaczył się restrykcjami rządowymi i przyznał, że 40-bitowy klucz nie daje wystarczających gwarancji bezpieczeństwa. Ktokolwiek mający dostęp do ponadprzeciętnej mocy obliczeniowej komputerów potrafi złamać zabezpieczenie siłową metodą prób i błędów. Klucz 40-bitowy stosowany może być tylko dla powszechnych operacji przekazywania numeru karty kredytowej. Netscape

obliczył, że czas komputerów potrzebny do złamania klucza ma wartość 10 000 USD, co czyni złamanie zwykłej transakcji zakupu kartą kredytową nieopłacalnym.

Netscape w amerykańskiej wersji swojej przeglądarki zastosował klucz 128 bitowy, znacznie bardziej odporny na złamanie metodą prób i błędów. Ale i to rozwiązanie nie okazało się w pełni bezpieczne. We wrześniu 1995 roku dwóch studentów pierwszego roku studiów dyplomowych Berkley University opracowało metodę, przy użyciu której na pojedynczej stacji roboczej w ciągu maksymalnie kilku godzin łamali wiadomość zakodowaną 128-bitowym kluczem. Studenci odkryli słaby punkt w zasadniczym dla szyfrowania algorytmie generatora liczb losowych. Okazało się, że liczby te nie były całkowicie losowe, zastosowany algorytm miał znacznie zaniżoną liczbę możliwych kluczy. Studenci byli w stanie zawęzić liczbę testowanych wartości do stosunkowo małej liczby. Pozwoliło im to na odszyfrowywanie niektórych wiadomości w kilka sekund. Obliczyli, że tak naprawdę 128-bitowy klucz oferuje w najlepszym wypadku realne szyfrowanie o długości 47 bitów. Netscape wypuścił natychmiast poprawioną wersję swojej przeglądarki. Dodatkowo opublikował specyfikację użytego przez siebie algorytmu generacji klucza.

Z tych wypadków można wysnuć szereg wniosków. Niespodziewane złamanie zabezpieczeń Netscape'a możliwe było dzięki temu, że Netscape, troszcząc się o zachowanie sekretów firmy, nie opublikował uprzednio specyfikacji swoich rozwiązań. Wynika z tego, że nie należy ufać utajnionym algorytmom, jako że ktoś może je kiedyś poznać i złamać. Prawdziwie bezpieczne rozwiązanie powinno być dostępne na poziomie dokładnej specyfikacji dla wszystkich. O jego bezpieczeństwie świadczyć będzie odporność na ciągłe próby złamania przez niezależnych ekspertów. Algorytm może być uważany za bezpieczny tak długo, jak nie zostanie pokonany. Jest to najważniejsze kryterium jego prawdziwej wartości.

SSL jest protokołem otwartym. Specyfikacja SSL jest ogólnodostępna w Internecie, jej wykorzystanie do celów niekomercyjnych jest bezpłatne. Do zastosowań komercyjnych wymagana jest płatna licencja Netscape.

3.7.2. S-HTTP

S-HTTP oznacza Secure Hypertext Transfer Protocol i jest drugą po SSL metodą zabezpieczania dokumentów przesyłanych przez WWW. Opracowana została w 1994 roku przez Enterprise Integration Technologies[30] (EIT) jako rozszerzenie standardowego protokołu HTTP, języka wymiany danych w WWW. Komercyjna wersja S-HTTP opracowana została w 1994 roku przez Tetrisa Systems[31], wspólną firmę EIT i RSA Data Security.

S-HTTP działa na poziomie aplikacji, szyfrując przesyłane dane, wspomagana jest autentyfikacja nadawcy. Jako mechanizmy szyfrowania stosowane są zarówno mechanizmy klucza publicznego RSA, jak i kodowanie kluczem symetrycznym oraz mechanizm Kerberos. Aktualnie używany mechanizm ustalany jest pomiędzy stronami na początku każdej transakcji. Algorytmy szyfrujące zastosowane w S-HTTP to DES, dwu kluczowy i trzy kluczowy potrójny DES, DESX, IDEA, RC2 oraz CDMF.

S-HTTP i SSL na różny sposób rozwiązują bezpieczeństwo komunikacji w Internecie. Główną różnicą pomiędzy nimi jest poziom, na którym działają (modelu ISO-OSI). SSL operuje z poziomu transportu, S-HTTP z poziomu aplikacji. Oznacza to, że o ile przy zastosowaniu SSL szyfrowana jest cała komunikacja i stosowane mogą być dowolne aplikacje, o tyle S-HTTP wymaga aplikacji specjalne napisanej z uwzględnieniem tej specyfikacji i szyfruje każdą wiadomość niezależnie. S-HTTP umożliwia podpis elektroniczny dowolnej wiadomości, możliwości tej nie ma SSL. Oba systemy mogą działać razem poprzez zastosowanie S-HTTP ponad SSL. Wzmacnia to bezpieczeństwo transmisji.

3.7.3. PCT

Konkurentem SSL jest opracowany wspólnie przez Microsoft i Visa International protokół PCT (Private Communication Technology). Oczekuje on na standaryzację. Jest on bardzo podobny do SSL i do pewnego stopnia z nim kompatybilny. Główne usprawnienia to zastosowanie dodatkowych algorytmów szyfrujących, zmniejszenie ilości wymaganych wiadomości pomiędzy serwerem i klientem, wiadomości są też

[30] http://www.eit.com/
[31] http://www.terisa.com/

krótsze, bezpieczniejsza i pewniejsza autentyfikacja (przez zastosowanie kluczy większej długości niż do szyfrowania).

3.7.4. SET

Najnowszą (początek 1996 roku) inicjatywą w dziedzinie standardów elektronicznych transakcji internetowych jest SET (Secure Electronic Transactions). Jest to wspólny projekt rywalizujących ze sobą uprzednio potentatów branży kart kredytowych: Visa International i Mastercard International. Do niedawna Visa wspólnie z Microsoftem promowała za wszelką cenę PCT, a Mastercard razem z Netscape koncentrował się na SSL. Pomimo iż firmy oficjalnie deklarowały chęć współpracy i uczynienia swoich systemów wzajemnie kompatybilnymi, w praktyce nic z tego przez długi czas nie wychodziło. Istniała groźba, że powstaną dwa niezależne, odmienne systemy elektronicznych transakcji, co znakomicie utrudniłoby życie klientom i sprzedawcom. W końcu firmy doszły jednak do wniosku, że korzystniejsze będzie opracowanie wspólnego systemu, który będzie przyjęty przez rynek jako obowiązujący standard. Umowa gwarantuje, że żaden z partnerów nie zdominuje pozostałych wspólników. Specyfikacja SET dostępna jest dla wszystkich za darmo[32], co ma umożliwić niezależnym wytwórcom oprogramowania tworzenie kompatybilnych aplikacji.

SET zapewnia mechanizmy bezpiecznych rozliczeń za pomocą kart płatniczych poprzez WWW. Specyfikacja zawiera komunikaty służące do elektronicznego kupowania towarów i usług, wspiera żądania autoryzacji płatności i certyfikatów. Podpisy, numery kart płatniczych oraz klucze symetryczne szyfrowane są metodą klucza publicznego algorytmem RSA, główna transmisja szyfrowana jest DES.

3.7.5. Fortezza

Popularnie stosowane mechanizmy bezpieczeństwa, takie jak SSL i S-HTTP, nie są wystarczające dla szczególnie wymagających klientów takich jak wojsko, wymiar sprawiedliwości, dyplomacja etc. Dla takich instytucji bardzo istotne jest nie tylko szyfrowanie danych, ale także stuprocentowa autentyfikacja. Odpowiedzią na ich potrzeby jest mechanizm nazywany Fortezza. Do masowego szyfrowania używa ona 56 bitowego DES (w przeciwieństwie do 40 bitowych kluczy w SSL i PCT). Użytkownicy

[32] http://www.visa.com; http://www.mastercard.com

mają swoje konta i hasła, ale kluczowym elementem zabezpieczającym są karty chipowe PCMCIA, przechowujące unikalny kod identyfikacyjny użytkownika. Aby posługiwać się kartą, należy znać jej kod autoryzujący PIN. Każdy z użytkowników Fortezzy ma swoją własną kartę. Karty sprzężone są z komputerami poprzez czytniki kart. Bezpieczne przeglądarki WWW mają swoje rozszerzenia umożliwiające korzystanie z Fortezzy.

Fortezza jest standardem agend rządowych USA. Gwarantuje to zainteresowanie tym systemem prywatnych dostawców, liczących na lukratywne rządowe kontrakty. Przykładowo Netscape już ogłosił swoje wsparcie dla Fortezzy w ramach rozszerzania SSL.

3.7.6. Bezpieczna poczta elektroniczna

Znaczenie szczególne ma bezpieczeństwo poczty elektronicznej, która jest najczęściej używaną usługą internetową. Jednym z mechanizmów mających zapewnić jej bezpieczeństwo jest PEM (Privacy Enhanced Mail), standard oficjalnie zaproponowany, ale jeszcze nie przyjęty. Zawiera mechanizmy szyfrowania zarówno symetrycznego jak i asymetrycznego, zarządzanie kluczami, autentyfikację-elektroniczny podpis. Dotychczas wspiera tylko algorytm DES, inne mają zostać dodane później. Dodatkowo zaproponowana została rozszerzająca wersja PEM-MIME zwana także MOSS (MIME Object Security Standard), która integruje PEM z powszechnie używanym do przesyłania poczty elektronicznej standardem MIME (Multipurpose Internet Mail Extensions). MIME umożliwia przesyłanie pocztą wiadomości o dowolnym formacie, w tym bogatego formatowania tekstu, grafiki i dźwięku. Konkurentem PEM i MOSS w dziedzinie bezpiecznej poczty elektronicznej jest S/MIME (Secure/Multipurpose Internet Mail Extensions), który bazując na MIME dodaje podpis elektroniczny i szyfrowanie wiadomości. Standard ten jest popierany przez wiele czołowych firm komputerowych.

3.8. PODSUMOWANIE

Autentyfikacja, autoryzacja i płatność może następować on-line albo off-line. Autoryzacja off-line ma kosztowniejsze niż on-line wymagania sprzętowe. Zarówno po

stronie klienta (karta chipowa), jak i sprzedającego (terminal POS) potrzeba urządzeń odpornych na włamywanie się i fałszowanie czy kradzież danych. Systemy on-line, pomimo większych wymagań komunikacyjnych, występują w Internecie częściej. Technologie zapewniające szyfrowanie i autentyfikację są dostępne od lat. Niemniej jednak handel internetowy dalej nie jest w pełni bezpieczny. Udowadnia to, że sama technologia to nie wszystko. Wymagana jest odpowiednia infrastruktura i całościowe podejście do problemu, w którym szyfrowanie stanowi zaledwie część rozwiązania.

Elementem często pomijanym są systemy komputerowe sprzedawcy i kupującego. System sprzedawcy to zwykle serwer internetowy, oparty na którymś z popularnych, komercyjnych systemów operacyjnych (najczęściej jedna z odmian UNIX'a). Systemy te nie są niezawodne. Wielokrotnie się do nich włamywano. Jeśli poufne dane (adresy klientów, numery kart kredytowych, szczegóły transakcji, numery kont bankowych etc.) przechowywane są bezpośrednio na tym samym serwerze w nie zaszyfrowanych plikach czy bazie danych, to cała skomplikowana technologia szyfrowania na nic się nie przydaje. Zamiast łamać algorytmy szyfrujące, złodziej włamuje się po prostu do serwera. Aby temu zapobiec, należy zwracać dużą uwagę na bezpieczeństwo lokalnego systemu, co jest bardzo dokładnie opisane w literaturze przedmiotu. Można stosować specjalne, dodatkowo zabezpieczone wersje systemów operacyjnych, szyfrować informacje w bazie danych, umieścić system za zasłoną ogniową (firewall). Firewall jest bodajże najczęściej stosowanym zabezpieczeniem internetowym. Może filtrować ruch w sieci pod kątem adresów IP, blokując wewnętrznym użytkownikom dostęp do Internetu i zewnętrznym dostęp do wewnętrznej sieci korporacyjnej- Intranetu. Może to polegać na umożliwieniu pracownikom korzystania tylko z poczty elektronicznej (odcięciu innych usług internetowych). Zewnętrzni użytkownicy, poza określonymi osobami zaufanymi, są najczęściej odcięci od wewnętrznej sieci LAN w całości. Firewall ochrania w ten sposób wewnętrzny system komputerowy i redukuje niepotrzebny ruch w sieci.

Rozpowszechnienie się Internetu spowoduje, że użytkownicy będą chcieli korzystać z niego z wielu publicznych komputerów. Oznacza to, że wszelkie rozwiązania oparte na hasłach czy kodach szyfrujących nie dają stuprocentowej gwarancji bezpieczeństwa. Dane narażone są na przechwycenie, zawsze bowiem urządzenie wejściowe może być

tak zmodyfikowane, aby pamiętało wprowadzane ciągi znaków, które potem mogą zostać odczytane przez złodzieja. Rozwiązaniem może być zastosowanie kodów jednorazowych, generowanych przez specjalne urządzenie. W połączeniu z kodem szyfrującym i hasłem dawałoby to autentyfikację użytkownika. Przechwycenie takiego kodu nie byłoby groźne, jako że zmieniałby się on przy każdej dokonywanej transakcji.

Dodatkowo sama stacja robocza może zostać tak przeprogramowana, by dokonywać nie autoryzowanych zakupów na koszt aktualnie z niego korzystającego użytkownika. Także komputery domowe, z których korzysta tylko właściciel, nie są do końca bezpieczne. Łatwo zaprogramować wirusa, kradnącego hasła i przesyłające je przez modem do włamywacza.

Lepsze bezpieczeństwo daje zastosowanie karty chipowej, wkładanej do czytnika kart podłączonego do komputera lub gniazda PCMCIA. Karta jest tak skonstruowana, że nie można odczytać w sposób nie autoryzowany zapisanych na niej informacji (klucza szyfrującego i hasła użytkownika). Ze względu na relatywnie wysokie bezpieczeństwo i wygodę będzie to zapewne w najbliższym czasie preferowana metoda płatności Internetowych.

Ponieważ jednak czytnik karty także może być potencjalnie przeprogramowany w ten sposób, aby dokonywać nie autoryzowanych transakcji, najbezpieczniejszym rozwiązaniem wydają się prywatne przenośne elektroniczne portfele, gwarantujące poprawne wykorzystanie zapisanych na karcie chipowej elektronicznych pieniędzy.

Jeśli chodzi o bezpieczeństwo danych przesyłanych siecią, to aktualnie stosowane algorytmy uważa się za bezpieczne. O ile sam algorytm nie zawiera błędu, dane nim zaszyfrowane przy długości klucza większego niż 56 bity są trudne do złamania. Przeszkodą w szerszym stosowaniu kryptografii są ograniczenia rządu amerykańskiego, obawiającego się, że zbyt zaawansowane techniki kryptograficzne uniemożliwią mu legalną inwigilację kryminalistów i terrorystów. Technologie stosujące zaawansowaną enkrypcję uważane są przez rząd Stanów Zjednoczonych za strategiczne i podlegają takim samym ograniczeniom eksportowym jak nowoczesna broń. Europejskie wersje amerykańskiego oprogramowania mają wyeliminowane lub poważnie ograniczone

funkcje kryptograficzne. Przykładowo Netscape Navigator ma enkrypcję ograniczoną do 40-bitowego klucza kodującego dla zastosowanego w mechanizmie SSL algorytmu RC4. Wyłącznie amerykańska wersja tego samego produktu ma znacznie bezpieczniejszy klucz 128-bitowy. Całkowity zakaz eksportu bądź reeksportu obowiązuje w stosunku do Kuby, Iraku, Libii, Płn. Korei, Iranu, Syrii i innych krajów objętych amerykańskimi restrykcjami.

Nad uczynieniem Internetu bardziej bezpiecznym i przystosowaniem go do potrzeb internetowego handlu pracuje wiele firm i organizacji o uznanym autorytecie i wkładzie w rozwój Internetu. Nad rozwiązaniami mającymi dodać mechanizmy bezpieczeństwa na poziomie IP pracuje Internet Engineering Task Force. Ma to zapewnić autentyfikację (nie na poziomie pojedynczych użytkowników) i szyfrowanie komunikacji pomiędzy komputerami. Wypracowaniem respektowanych przez wszystkich standardów zajmuje się World Wide Web Consortium[33].

[33] http://www.w3.org/pub/WWW/

ZAKO□CZENIE

Handel przez Internet jest już faktem. Ocenia się, że działalność komercyjną za pośrednictwem Internetu prowadzi obecnie ponad 25 000 firm. Wartość internetowych transakcji w roku 1995 to około 500 milionów USD, ma ona wzrosnąć od 2 do 5 miliardów USD w roku 2000[34]. O ile dotychczas Internet używany był przez firmy głównie do komunikacji z klientem, to obecnie w coraz większym stopniu wykorzystywany jest do zawierania transakcji i sprzedaży on-line.

Znaczenie Internetu będzie rosło we wszystkich sferach działalności gospodarczej: w sprzedaży detalicznej, w kontaktach pomiędzy firmami, w bankowości. Firmy, które pierwsze i najszerzej zainwestują w działalność za pośrednictwem Internetu, odniosą z niego największe korzyści w przyszłości. Szczególna rola przypadnie występującym często w płatnościach internetowych organizacjom pośredniczącym pomiędzy kupującym, sprzedającym a instytucją finansową. Ich rola jest analogiczna do funkcji firmy telekomunikacyjnej czy przedsiębiorstwa pocztowego w handlu konwencjonalnym. Zapewniają płynność i sprawne funkcjonowanie technicznej infrastruktury handlu internetowego. Są mediatorem i dostarczycielem rozwiązań obejmujących swym zakresem sprzęt, oprogramowanie i sposób posługiwania się Internetem. Ich istnienie pozwala sprzedającym skupić się na prowadzeniu interesów.

Internet jest szansą dla małych sprzedawców. Przy znikomych opłatach będą oni w stanie zaoferować swoje towary i usługi milionom sieciowych użytkowników. Może to doprowadzić do wytworzenia się całkiem nowego elektronicznego rynku towarów i usług, w którym najmniejsi sprzedawcy będą kogli koegzystować, a nawet konkurować z olbrzymimi korporacjami.

Handel elektroniczny oparty jest przede wszystkim na globalnej pajęczynie World Wide Web. Technologia ta, jak i cały Internet ciągle się rozwija. Dodawane są nowe usługi i standardy. Zawartość serwisów WWW jest coraz atrakcyjniejsza graficznie i w rosnącym stopniu mutimedialna. Handel podąża krok w krok za nowinkami technologicznymi i oferuje coraz ciekawszą ofertę, np. trójwymiarowe katalogi

towarów. Jego rozwój hamowany jest jednak przez nie wykształcone jeszcze w pełni mechanizmy płatności poprzez Internet. Aczkolwiek w ciągu ostatnich 18 miesięcy pojawiło się wiele interesujących propozycji, internetowe płatności są dalej w fazie wczesnego rozwoju. Świadectwem tego są popełniane błędy. Włamywacze przechwytywali nie szyfrowane wiadomości nadawane siecią. Teoretycznie bezpieczne algorytmy szyfrowania były łamane, włamywano się do systemów komputerowych banków.

Żaden z istniejących systemów płatności nie zdobył dotychczas absolutnej dominacji. Jest wysoce prawdopodobne, że w ciągu najbliższych 1-2 lat na rynku pozostanie kilka uzupełniających się wzajemnie rozwiązań. Wartość i częstość zachodzenia transakcji pociąga za sobą różne wymagania co do bezpieczeństwa i kosztów transakcyjnych. Transakcje o dużej wartości realizowane będą zapewne na bazie którejś z metod wykorzystujących kartę kredytową czy czek. Mikro i średniej wielkości płatności realizowane mogą być kartami chipowymi. Ich szersze zastosowanie wymaga jednak upowszechnienia tanich i niezawodnych czytników kart, podłączanych do komputera. Do tego czasu popularne będą czysto softwarowe rozwiązania elektronicznych pieniędzy i portfeli.

Ostatecznie mechanizmy płatności internetowych połączą się z płatnościami pozasieciowymi dokonywanymi przy użyciu podręcznych elektronicznych portfeli z kartami chipowymi jako nośnikami pieniędzy. Oferują one największą wygodę i bezpieczeństwo. Wyposażone będą w miniklawiatury, wyświetlacz i moduły komunikacji z kompatybilnymi urządzeniami poprzez podczerwień. Elektroniczne portfele integrować będą zapewne także inne funkcje- osobistego komunikatora, (łączącego wideotelefon, pocztę elektroniczną, przeglądarkę WWW) i elektronicznego asystenta.

Do wzrostu popularności jednych rozwiązań kosztem drugich przyczynić się mogą dodatkowo względy kulturowe i ograniczenia instytucjonalne narzucone przez rządy obawiające się np. łatwości prania brudnych elektronicznych pieniędzy.

[34] Banking Technology, 1995

Musi upłynąć jeszcze kilka lat, zanim systemy płatności okrzepną na tyle, by można ich było używać na skalę masową. Będzie to zapewne skorelowane w czasie z jeszcze większym poszerzeniem bazy użytkowników Internetu, którzy zaczną z niego korzystać poprzez łącza telewizji kablowej i zintegrowane domowe centra komunikacyjne. Powszechny handel elektroniczny będzie integralną częścią infostrady, która zapewne już niedługo dotrze do naszych domów.

Spis wykresów

Spis rysunków

S□ownik poj□□

ACH- Automated Clearing House, amerykański system elektronicznego transferu pieniędzy.

ARPANET- eksperymentalna sieć stworzona w latach 60 w USA- protoplastą dzisiejszego Internetu.

Autentyfikacja- możliwość stwierdzenia, czy dany użytkownik sieci naprawdę jest tym, za kogo się podaje.

CDMF- algorytm szyfrujący zastosowany w S-HTTP.

CERN- Conseil Europeen pour la Recherche Nucleaire, instytut badań jądrowych w Szwajcarii i Francji, miejsce narodzin WWW.

Cyberbuck- nazwa testowego pieniądza elektronicznego firmy DigiCash.

CyberCash- amerykańska firma, dostawca jednego z systemów internetowych płatności.

DES- Data Encryption Standard, algorytm szyfrowania symetrycznego, oficjalnie przyjęty jako standard przez rząd USA.

DESX- wariant DES.

DigiCash- amerykańska firma, dostawca jednego z systemów internetowych płatności, opartego na elektronicznych pieniądzach.

E-cash electronic cash, elektroniczne pieniądze.

EDI- Electronic Data Interchange, metoda elektronicznej wymiany informacji handlowej między komputerami.

EFT- Electronic Funds Transfer, elektroniczny przekaz środków pieniężnych przez banki.

Email- poczta elektroniczna, system przesyłania wiadomości między użytkownikami Internetu.

FDIC- Federal Deposit Insurance Corporation - organizacja ubezpieczającą depozyty bankowe w USA.

Finger- usługa internetowa umożliwiająca użytkownikom zasięganie informacji o innych użytkownikach/ komputerach w Internecie.

Firewall-kombinacja sprzętowo-programowa separująca sieć lokalną od Internetu.

Fortezza- metoda bezpiecznej komunikacji internetowej; karta PCMCIA z zaimplementowanym algorytmem Capstone.

FTP- File Transfer Protocol, protokół definiujący sposób transmisji plików pomiędzy komputerami w Internecie, także program realizujący taką transmisję.

Gopher- hierarchiczny system dystrybucji informacji w Internecie, obecnie wypierany przez WWW.

Hipertekst- tekst w dokumencie zawierający połączenia do innych dokumentów, powodujące, że po ich wybraniu dokumenty te zostaną wczytane i wyświetlone; metoda dystrybucji informacji w WWW.

HTTP- Hypertext Transfer Protocol, protokół transmisji dokumentów hipertekstowych w WWW.

IDEA- International Data Encryption Algorithm, algorytm szyfrowania symetrycznego.

iKP- Internet Keyed Payments, protokół płatniczy opracowany przez firmę IBM.

IRC- Internet Relay Chat, usługa Internetowa, dzięki której rozmawiać ze sobą może wielu użytkowników naraz.

Kerberos- usługa autentyfikacyjna oparta na szyfrowaniu symetrycznym.

MD5- algorytm kompresji wiadomości używany w elektronicznym podpisie.

MIME- Multipurpose Internet Mail Extensions, rozszerzenie poczty internetowej o możliwość przesyłania plików.

Mosaic- pierwsza graficzna przeglądarka WWW.

MOSS- MIME Object Security Standard, standard bezpiecznej poczty elektronicznej.

NCSA- National Center for Supercomputing Applications, centrum badań naukowych w USA, miejsce powstania przeglądarki WWW Mosaic.

NetBill- jedna z technologii internetowych płatności.

NetCash coupons- nazwa elektronicznych pieniędzy w systemie NetCash.

NetCash- jedna z technologii internetowych płatności bazująca na elektronicznych pieniądzach.

NetCheque- jedna z technologii internetowych płatności.

Netscape Navigator- najpopularniejsza obecnie na rynku przeglądarka WWW.

PCT- Private Communication Technology, metoda szyfrowania wiadomości przesyłanych przez WWW.

PEM- Privacy Enhanced Mail, standard bezpiecznej poczty elektronicznej.

PGP (Pretty Good Privacy)- popularny w Internecie standard bezpiecznej poczty elektronicznej.

Potrójny DES- odmiana algorytmu DES.

Przeglądarka WWW- program umożliwiający korzystanie z zasobów WWW.

RC2- metoda szyfrowania symetrycznego.

RC4- metoda szyfrowania symetrycznego.

RSA- popularny system szyfrowania metodą klucza publicznego.

S/MIME- standard bezpiecznej poczty elektronicznej.

Secure Courier- zaproponowany przez Netscape Corp., protokół bezpiecznego handlu internetowego.

Secure Netscape- jedna z technologii internetowych płatności bazująca na kartach kredytowych.

SET (Secure Electronic Transactions)- proponowany mechanizm bezpiecznych rozliczeń za pomocą kart płatniczych poprzez WWW.

SHA- Secure Hash Algorithm, jeden z algorytmów stosowany w elektronicznym podpisie.

S-HTTP Secure Hypertext Transfer Protocol, metoda szyfrowania danych przesyłanych przez WWW.

SMTP- Simple Mail Transfer Protocol, podstawowy standard poczty elektronicznej w Internecie.

SSL- Secure Sockets Layer, opracowany przez Netscape Corp. bezpieczny sposób szyfrowania danych przesyłanych przez WWW.

TCP/IP- Transmission Control Protocol/Internet Protocol, zespół protokołów na których oparty jest Internet.

TELNET- protokół umożliwiający logowanie się poprzez Internet do innych systemów komputerowe; program realizujący taką usługę.

URL- Uniform Resource Locator, znormalizowany sposób adresowania zasobów w Internecie.

USENET- zdecentralizowany system grup dyskusyjnych w Internecie.

VirtualPIN- identyfikator użytkownika zastępujący numer karty kredytowej w internetowym systemie płatności First Virtual.

WAIS- Wide Area Information Servers, system indeksowania zasobów internetowych.

WWW- W3- World Wide Web- globalna pajęczyna, hipertekstowy, rozproszony system dystrybucji informacji w Internecie.

Bibliografia

Informacje o Internecie

http://www.commerce.net/
gopher://ds1.internic.net/00/fyi/fyi20.txt
http://is.internic.net/
http://www.w3.org/pub/WWW/
http://www.isoc.org/
http://www.economist.com/surveys/internet/index.html

Statystyki wykorzystania Internetu

http://www.clark.net/pub/granered/demo.html
http://etrg.findsvp.com/
http://www.cyberatlas.com/
http://www.cc.gatech.edu/gvu/user_surveys/survey-10-1995/
http://www-personal.umich.edu/~sgupta/hermes/
http://www.nw.com/
http://www.europay.com/1995/ph5rtt45.htm

Handel elektroniczny w Internecie

http://www.sims.berkeley.edu/resources/infoecon/Commerce.html#cash
http://cism.bus.utexas.edu/ec.html
http://www.w3.org/hypertext/WWW/Payments/roadmap.html
http://www.ecs.hosting.ibm.com/links/index.html
http://www.ex.ac.uk/~RDavies/arian/emoney.html
http://www.moneypage.com/emoney/
http://www.pitt.edu/~malhotra/Elecomm.htm
http://www.yahoo.com/Business_and_Economy/Electronic_Commerce/
http://www.intermarket.com/ecl/
http://www.netresource.com/itp/cari.html
http://www.clickshare.com/clickshare/
http://www.cwi.nl/cwi/projects/cafe.html
http://www.cox.smu.edu/mis/cases/webcase/commerce.html
http://www2000.ogsm.vanderbilt.edu/webcase/home.html
http://www.virtualschool.edu/mon/ElectronicMoney.html
http://www.isworld.org/isworld/ecourse/isw34111.html
http://ganges.cs.tcd.ie/mepeirce/project.html
http://www.ecworld.org/welcome.html
http://www.euro.net/innovation/ift/BizRep/BusIntTC.htm

http://www.netfare.com
http://www.research.digital.com/SRC/personal/steveg/millicent/millicent.html
http://www.sims.berkeley.edu/resources/infoecon/Commerce.html#cash
http://www.geocities.com/WallStreet/1203/#b
http://gnn.com/meta/finance/feat/emoney.home.html
http://www.research.att.com/lateinfo/projects/ecom.html
http://www.cs.cmu.edu/afs/cs.cmu.edu/user/jeanc/www/usenix.html
http://e-comm.iworld.com/
http://commerce.anu.edu.au/comm/staff/RogerC/Electronic_Commerce/
http://www.research.att.com/jsac/prot/jsac13.8/neuman/neuman.html
http://snad.ncsl.nist.gov/dartg/edi/arch.html
http://www-iwi.unisg.ch/iswnet/ec_em.html
http://www.isoc.org/in95prc/HMP/PAPER/136/html/paper.html
http://www.zurich.ibm.ch/Technology/Security/publications/1995/
http://www.usc.edu/dept/ATRIUM/Papers/EC_on_the_Inet.html

Elektroniczna Wymiana Danych (EDI)

http://commerce.anu.edu.au/comm/staff/RogerC/Electronic_Commerce/
http://www.editie.nl
http://www.premenos.com/Resources/periodicals/edi_forum/article.html
http://www.ecworld.org/Resource_Center/Case_Studies/hornback.html
http://catalog.com:80/napmsv/edi.htm
http://ganges.cs.tcd.ie/4ba2/edi/index.html
http://www.ecworld.org/Help/bcmenu.html
http://www.ecrc.gmu.edu/edistone/ediqztop.html

Internet banking

http://www.corpfinet.com/TopTen.html
http://www.netchex.com/index.html
http://www.cib.org.uk/banks.html
http://www.sfnb.com/
https://banking.wellsfargo.com/more_on.html
http://www.canadatrust.com/ct/pcbank/pchb.html
http://bankswith.apollotrust.com/www/banking.html
http://www.advance.com.au/advance/ibank.htm
http://www.marktwain.com/

Internetowe systemy płatności

http://www.cybercash.com/
http://www.mastercard.com

http://www.fv.com/
http://www.gctec.com/
http://www.worldserver.pipex.com/mondex/
http://www.digicash.nl/
http://www.openmarket.com
http://www.teleport.com/~netcash/
http://www.visa.com.
http://www.checkfree.com/
http://www.europay.com/electcom.htm
http://nii-server.isi.edu/info/NetCheque/
http://www.ini.cmu.edu/netbill/
http://www.verisign.com/
http://home.netscape.com/newsref/ref/netscape-security.html
http://www.checkmaster.com/index.html

Bezpieczeństwo w Internecie

http://www.ov.com/misc/krb-faq.html
http://gost.isi.edu/info/kerberos/
http://www.netscape.com/newsref/ref/netscape-security.html
http://www.v-one.com/pubs/attacks/1.htm
http://www.v-one.com/pubs/fw-faq/faq.htm
http://www.rsa.com/
http://www.commerce.net/information/standards/drafts/shttp.txt
http://home.mcom.com/info/SSL.html
http://ds.internic.net/internet-drafts/draft-ietf-http-digest-aa-01.txt
http://www.zurich.ibm.com/Technology/Security/extern/ecommerce/
http://www.ibm.com/security/
http://www.commerce.net/information/services/security.html
http://www.w3.org/pub/WWW/Security/
http://www.advance.com.au/advance/security.htm
http://www.secureware.com/
http://www.eit.com/cgi-bin/textit/creations/s-http/index.html
http://www.commerce.net/directories/jumpstation/protocol.html
http://www.commerce.net/information/position/position.062695.html